EXHIBIT A

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Executive Summary

1. During the course of several analyses on behalf of Fortune 500 advertisers, impression level log file data and financial invoices suggested that advertisers were billed by ad tech vendors for ad impressions served to declared bots operating out of known data center server farms. Some of these bots are on the IAB Tech Lab Bots & Spider List, and some of the data center IP addresses are on an industry reference list of known datacenter IPs with non-human (bot) traffic.
    a. Some of these brands reported that they were spending millions of dollars each year specifically for "bot avoidance" pre-bid segments and technology from various ad verification vendors. This technology is allegedly intended to prevent advertisers' ads from being served to bots, invalid, or fraudulent traffic.
2. Adalytics obtained access to three different web visitation datasets generated entirely by bots. The cumulative size of these internet crawling bot datasets is over a petabyte of web traffic data, with more than two million different websites crawled, and more than seven years worth of crawling data. The data includes web crawling sessions bots based in the USA, Canada, Latin America, Europe, Singapore, Australia, New Zealand, and Japan.
    a. All three of the bot datasets crawl the web for "benign" reasons, such as academic research or cybersecurity. None of these three bots is designed to commit "ad fraud" or intentionally generate ad revenue or invalid traffic. The

archiving bots run and access the Internet from data centers. Some of the bots announce themselves by declaring a known bot user agent. This enables web sites, ad tech vendors, and verification vendors to know upfront who or what is requesting their services and where the traffic originates from.

3. Some ad tech vendors appear to be serving audience targeted or "personalized" ads (including retargeting ads) to bots in data centers that have no stateful attributes, cookies, session storage, fingerprints, user IDs, or browsing history.
4. These bot datasets reveal that thousands of different brands - including Procter & Gamble, Hershey's, HP, Wall Street Journal, T-Mobile, United States Postal Service, Pfizer, IBM, JPMorgan Chase, Bank of America, Microsoft, Haleon, Australian Defence Force, New York, Utah, Oregon, Florida, Indiana & Virginia state governments, Bayer Healthcare, MasterCard, Ernst & Young, Visa, Kenvue, Pfizer, US Bank, Unilever, Disney, American Express, Beam Suntory, Diageo, and United States government agencies such as the New York City Police (NYPD), Department of Homeland Security (DHS TSA), US Census, healthcare.gov, US Army, US Air Force, US Navy, Department of Veterans Affairs, and the Centers for Disease Control and Prevention - had their ads served by ad tech vendors to bots in data centers for at least 5+ years (since at least 2020).
5. Many of these ads which were served to bots appear to be using various "pre-bid" bot avoidance or filtration tools from vendors such as Integral Ad Science (IAS) and DoubleVerify. For example, the US Navy had ads served to declared bots running out of Google Cloud server farms, whereas the US Navy's ads contain source code references to "charge-allDoubleVerifyBotAvoidance".
6. In just the observed sample dataset, Google was observed serving thousands of healthcare.gov ads (from the U.S. Centers for Medicare & Medicaid Services) for years to bots running out of data center server farms.
7. Many of the ad tech platforms which were observed serving ads to declared bots in data center server farms have declared publicly that they filter bot traffic pre-bid through partnerships with HUMAN Security (f/k/a "White Ops"). For example, Google, Trade Desk, Pubmatic, Magnite, Index Exchange, Triplelift, OpenX, Microsoft Xandr, Kargo, GumGum, Media.net, Sonobi, and Equativ

(f/k/a Smart AdServer) have made public statements about partnering with HUMAN Security to prevent ads from being served to bots. Additionally, some of these ad tech vendors also have announced partnerships with DoubleVerify and IAS.

   a. Trade Desk and Google's own ads promoting their own products or services were observed serving to these bots.

8. Some advertisers such as the Government of Ontario, Canada and Progressive (insurance) appear to be utilizing DoubleVerify's Scibids to target their ads. Scibids is a subsidiary that allegedly uses AI to target ads. It appears that some of these DoubleVerify Scibids-targeted ads were served to declared bots with no long term cookies or user IDs running out of data center server farms.
   a. Ads promoting Scibids' own products were served to bots with no pre-existing user IDs by Google
9. IAS's publisher services pixel appears to label declared bots (whose user agents are on the IAB Tech Lab Spiders and Bots list since 2013) running out of known data center server farms as valid, human traffic 17% of the time (meaning for every 100 declared bots observed herein, IAS labels 17 bot page view sessions as valid, human traffic). For non-declared bots operating out of data centers or other IPs, IAS's pixel appears to label the bot traffic as valid, human traffic 77% of the time in the observed sample dataset.
   a. In some cases, it appears that IAS' publisher optimization tool labeled the same bot and page view session as both valid, human traffic ("fr=false") and simultaneously as invalid, bot traffic ("fr=true").
   b. Furthermore, in some cases, even when IAS' publisher optimization tool identified a given user as a bot, there were still ads served to the bot on behalf of advertisers who appeared to be using IAS' advertiser-side tools.
10. Many premium publishers and ad tech industry trade press websites were observed serving ads to bots. For example, the trade press adweek.com and adage.com were observed serving Trade Desk ads promoting Trade Desk's own services to bots. Many publishers which appear to use IAS' and/or DoubleVerify publisher optimization tools - such as Wall Street Journal, Reuters, Fandom, Forbes, Weather.com, Condé Nast, and Washington Post - were observed serving major advertisers' ads to bots in data centers for years

11. Many media agencies were observed transacting clients' ads to declared bots on the IAB Tech Lab Spiders and Bots list running out of data center server farms. These included: GroupM / WPP, Interpublic Group (IPG), Dentsu, Publicis Groupe, Havas, Omnicom, Horizon Media, and MiQ.
12. Google Ad Manager (GAM) - a publisher ad server - was observed transacting millions of ad impressions from thousands of different advertisers to bots. Some of these bots were declared bots operating out of Google's own data center.
13. YouTube was observed serving TrueView skippable in-stream video ads for many different brands for years to bots running out of data center server farms - via the Google Video Partners (GVP) network. Some of these TrueView ads were served to declared bots operating out of Google Cloud data centers. Brands whose TrueView ads were served to bots include ads for Senator Mike Lee (R-UT), the Wall Street Journal, Miami-Dade County government Special Victims Bureau, Sexual Predator and Offender Unit (SPOU), Ernst & Young, Lego, Kelloggs, Kenvue (f/k/a J&J Consumer), Mercedes-Benz, and Visa.

Introduction

Over the course of the last year, Adalytics has conducted several research reports and worked with various public sector and Fortune 500 brand advertisers and media agencies to analyze their marketing data.

Several media buyers requested that Adalytics review their ad delivery data and/or log files generated by their advertising vendors. Some of these advertisers reported that they were paying several million dollars per year for bot avoidance pre-bid segments or technology. According to the advertisers, this technology was designed as an extra insurance policy to ensure that the advertisers' ads would not be served to bots or "invalid traffic" (industry jargon for ad delivery that does not conform with various industry standards and buyers' expectations, such as mis-declared or falsified ad placements).

The vendors providing this technology to advertisers, publishers and media agencies have various certifications from various advertising trade groups or accreditation bodies.

Despite paying for this technology, the brands were surprised to observe that their log files contained evidence that the brands had been charged and billed by their ad tech vendors for ads that were served to openly declared bots. Some brands reportedly saw that their ads were served to "Headless Chrome", various AI company crawlers and scrapers, and search engine crawlers. Some brands reportedly even had their ads served to a contextual classification bot operated by the very ad verification company the brands were paying millions of dollars to for bot avoidance.

In a few instances, it appeared that a verification vendor who was providing bot avoidance technology was marking significant percentages of an openly declared bot operating out of a known data center as valid, human traffic.

Furthermore, during the course of several research projects, Adalytics observed that the United States Navy, US Army, Centers for Disease Control and Prevention, Department of Veterans Affairs, and US Postal Service had their ads served to confirmed bots. Even members of Congress, such as Republican Senator Mike Lee, sponsor of the AMERICA Act, were observed as having their ads served to bots.

Prompted by these experiences and observations, the requests of numerous Fortune 500 brand marketing executives, and the public interest component of the United States government itself being affected, Adalytics decided to perform exploratory research to try to better understand the phenomenon of how ad tech vendors allow digital ads to be served to bots in data centers.

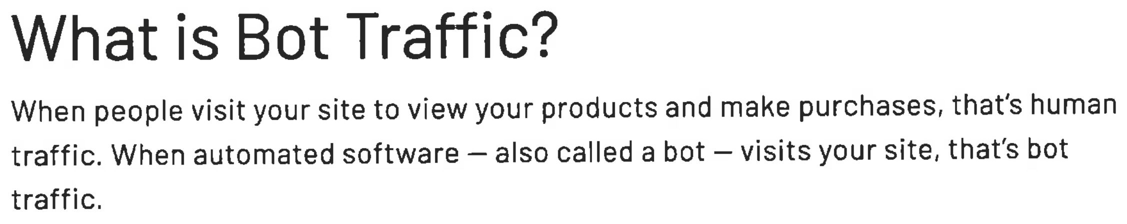
Background

This section of the report is intended to provide readers with background on what bots are, the prevalence of bot traffic on the open internet, various advertising industry jargon, advertising industry standards regarding ad delivery to bots, and prior research investigating the role of bot avoidance technology vendors.

What are bots, and how prevalent are they on the open internet ?

According to Cloudflare, a hosting company, "*Bot traffic describes any non-human traffic to a website or an app. The term bot traffic often carries a negative connotation, but in reality bot traffic isn't necessarily* *good or bad; it all depends on the purpose of the bots. Some bots are essential for useful services such as search engines and digital assistants (e.g. Siri, Alexa). Most companies welcome these sorts of bots on their sites. Other bots can be malicious, for example those used for the purposes of credential stuffing, data scraping, and launching DDoS attacks. Even some of the more benign 'bad' bots, such as unauthorized web crawlers, can be a nuisance because they can disrupt site analytics and generate click fraud."*

HUMAN Security, a company that provides technology to filter or block bots, states: "*When people visit your site to view your products and make purchases, that's human traffic. When automated software — also called a bot — visits your site, that's bot traffic."*



What is Bot Traffic?

When people visit your site to view your products and make purchases, that's human traffic. When automated software — also called a bot — visits your site, that's bot traffic.

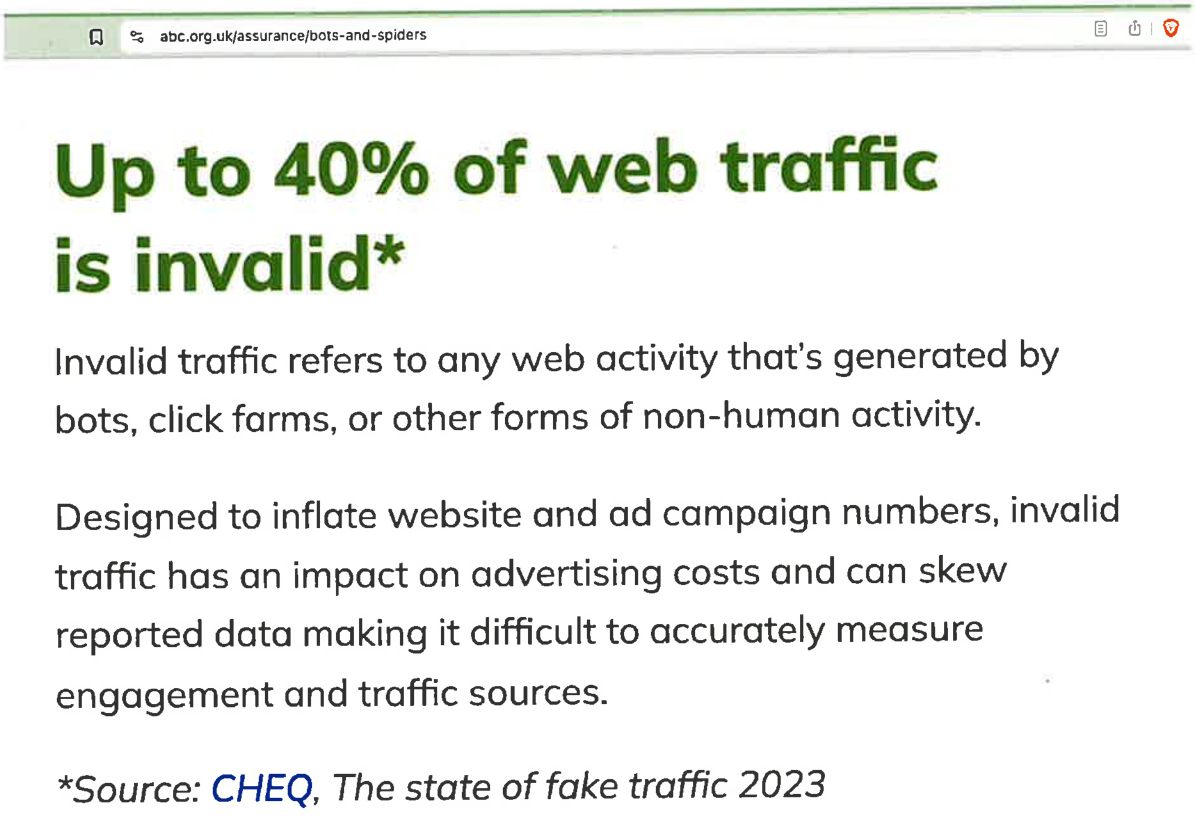
Source: HUMAN Security

Cloudflare further describes the negative consequences of bot traffic. Cloudflare states: "*unauthorized bot traffic can impact analytics metrics such as page views, bounce rate, session duration, geolocation of users, and conversions. These deviations in metrics can create a lot of frustration for the site owner; it is very hard to measure the performance of a site that's being flooded with bot activity. Attempts to improve the site, such as A/B testing and conversion rate optimization, are also crippled by the statistical noise created by bots [...] For sites that serve ads, bots that land on the site and click on various elements of the page can trigger fake ad clicks; this is known as click fraud."*

HUMAN Security states: *"Automated traffic taxes your infrastructure and increases your costs for bandwidth and compute cycles. Bot traffic can overwhelm your network and slow site performance, which frustrates customers and negatively impacts user experience [...] In addition, bot traffic contaminates your data and skews your analytics — for example, by appearing to show an increase in consumer demand. Flawed metrics* *on user behavior can lead you to make poor business decisions about pricing, stocking goods, and investing in marketing and advertising."*

Cloudflare further states: "*It is believed that over **40% of all Internet traffic is comprised of bot traffic, and a significant portion of that is malicious bots***" (emphasis added).

The website of the Audit Bureau of Circulations (ABC UK), a British non-profit that develops standards of media brand measurement, states that "*Up to 40% of web traffic is invalid [...] Designed to inflate website and ad campaign numbers, invalid traffic has an impact on advertising costs and can skew reported data making it difficult to measure engagement and traffic sources."*



Up to 40% of web traffic is invalid*

Invalid traffic refers to any web activity that's generated by bots, click farms, or other forms of non-human activity.

Designed to inflate website and ad campaign numbers, invalid traffic has an impact on advertising costs and can skew reported data making it difficult to accurately measure engagement and traffic sources.

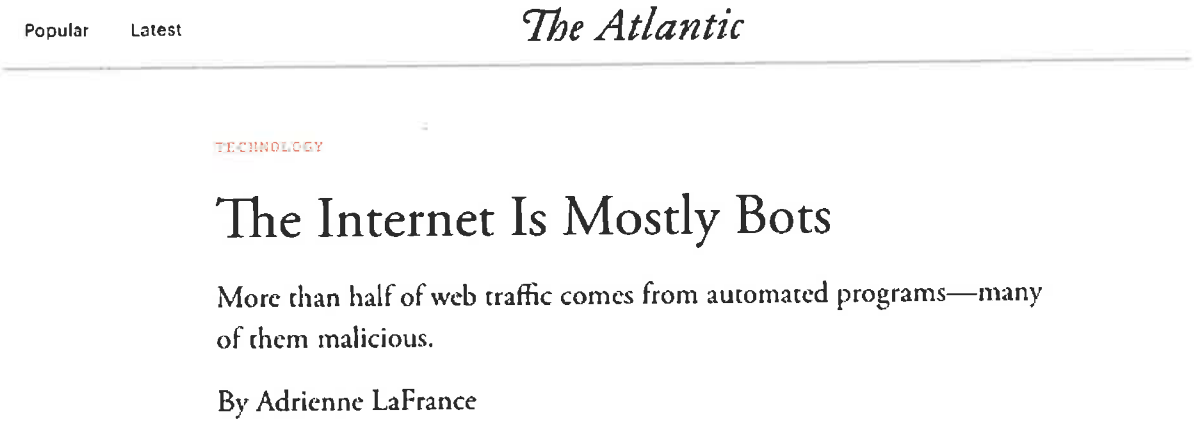
**Source: CHEQ*, *The state of fake traffic 2023*

Source: ABC UK and Cheq

The 2024 Imperva_Threat Research report "*reveals that almost 50% of internet traffic comes from non-human sources. Bad bots, in particular,* *now comprise nearly one-third of all traffic. Bad bots have become more advanced and evasive and now mimic human behavior in such a way that it makes them difficult to detect and prevent."*

According to Akamai Technologies research in June 2024, another hosting company, "*bots compose 42% of overall web traffic, and 65% of these bots are malicious.*"

According to The Atlantic, "*The Internet Is Mostly Bots - More than half of web traffic comes from automated programs—many of them malicious*", citing a 2017 study "*which is based on an analysis of nearly 17 billion website visits from across 100,000 domains.*"



Popular Latest

The Atlantic

TECHNOLOGY

The Internet Is Mostly Bots

More than half of web traffic comes from automated programs—many of them malicious.

By Adrienne LaFrance

Source: The Atlantic

Bot traffic can also increase the electricity consumption and Scope3 carbon emissions associated with advertisers media supply chains. According to a December, 2023 research report from company called Scope3 [which monitors carbon emissions associated with digital advertising], "*fraud in US programmatic display contributes an estimated 353k mt of carbon emissions.*"

Fraud in US programmatic display contributes an estimated 353k mt of carbon emissions

Source: Scope3

What is the estimated financial impact of bot traffic or ad fraud on digital advertising ?

In addition to the consequences of unfiltered bot traffic on web measurement and analytics, as well as on Scope3 carbon emissions, various entities have sought to estimate the financial impact of bot traffic or ad fraud on the digital advertising industry.

It bears mentioning that there are many forms of ad fraud beyond or outside of bot traffic. For example, one form of ad fraud may involve a vendor billing an advertiser for digital ads that were never served at all, or served to real humans but on a lower quality context than what was contractually agreed upon.

Different studies have tried to quantify the entire scale of ad fraud, or focused just on the subset of ad fraud related specifically to bot traffic. Furthermore, it is worth noting that not all bot traffic is fraudulent. For example, some bots have benign or beneficial activities, such as search engine crawling and indexing, or monitoring website quality. Readers should be careful not to assume that all bots are malicious or engineered specifically for the purpose of ad fraud. Bots can have beneficial functionality.

According to the World Federation of Advertisers (WFA), a trade group, *"Ad fraud likely to exceed $50bn globally by 2025 on current trends* *second only to the drugs trade as a source of income for organized crime."*

The Association of National Advertisers (ANA) published a study in 2017 that analyzed data collected from ten billion online ads purchased over a two-month period by 49 of the trade body's advertiser members. One advertiser allegedly had "served 37 per cent of its online ad campaign to bots".

The Association of National Advertisers (ANA) reported that "A false sense of security enables fraud to thrive."

In 2022, the ANA wrote that "*According to the results of a global 2019 study by Juniper Research, ad fraud costs the marketing industry an estimated $51 million per day, and these losses are likely to increase to $100 billion annually by 2023.*" The ANA also wrote that "*nearly 18 percent of all internet traffic in the marketing industry can be attributed to nonhuman bots, which are actively engaged in ad fraud.*"

Background - What is "invalid traffic" in ad tech industry jargon?

The Media Rating Council, an advertising industry accreditation body, published an "Invalid Traffic Detection and Filtration Standards Addendum" in 2020, defining "invalid traffic" (IVT).

The MRC's Standard Addendum states that: "Invalid Traffic (IVT) is defined generally as traffic or associated media activity (metrics associated to ad and content measurement including audience, impressions and derivative metrics such as viewability, clicks and engagement as well as outcomes) that does not meet certain quality or completeness criteria, or otherwise does not represent legitimate traffic that should be included in measurement counts. Among the reasons why traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.), or activity designed to produce IVT."

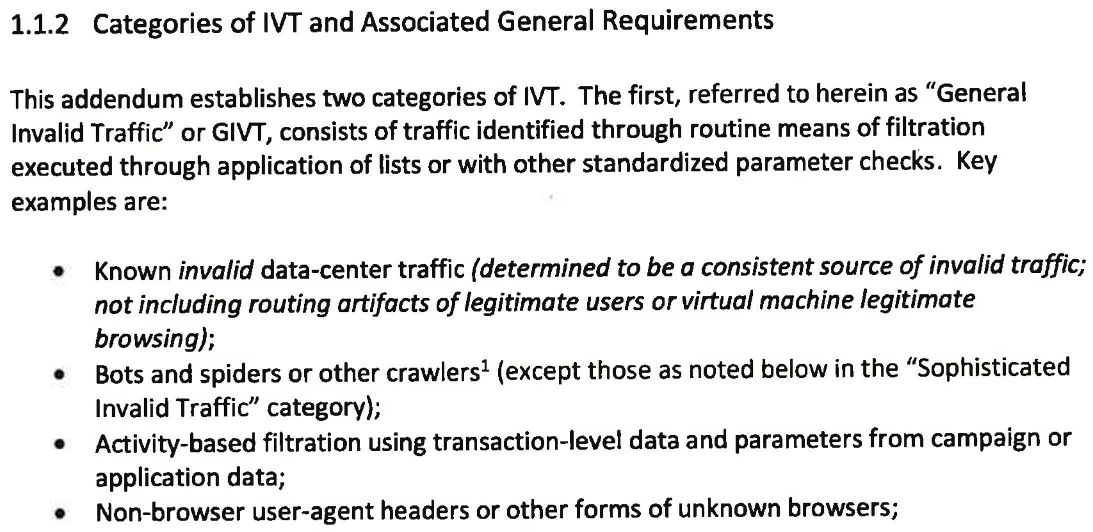
The MRC Addendum defines General Invalid Traffic (GIVT) and Sophisticated Invalid Traffic (SIVT).

The MRC Addendum states: "General Invalid Traffic" or GIVT, consists of traffic identified through routine means of filtration executed through application of lists or with other standardized parameter checks. Key examples are:

- Known invalid data-center traffic (determined to be a consistent source of invalid traffic; not including routing artifacts of legitimate users or virtual machine legitimate browsing);
- Bots and spiders or other crawlers (except those as noted below in the "Sophisticated Invalid Traffic" category);"
- "Non-browser user-agent headers or other forms of unknown browsers;"
- "Pre-fetch or browser pre-rendered traffic (where associated ads were not subsequently accessed by a valid user"

The MRC Addendum states that "the second category, herein referred to as "Sophisticated Invalid Traffic" or SIVT, consists of more difficult to detect situations that require advanced analytics, multi-point corroboration/coordination, significant human intervention, etc., to analyze and identify. Key examples are:

- Automated browsing from a dedicated device: Known automation systems (e.g., monitoring/testing), emulators, custom automation software and tools; [...]
- Bots and spiders or other crawlers masquerading as legitimate users detected via sophisticated means; [...]
- Invalid proxy traffic (originating from an intermediary proxy device that exists to manipulate traffic counts or create/pass-on invalid traffic or otherwise failing to meet protocol validation);"



1.1.2 Categories of IVT and Associated General Requirements

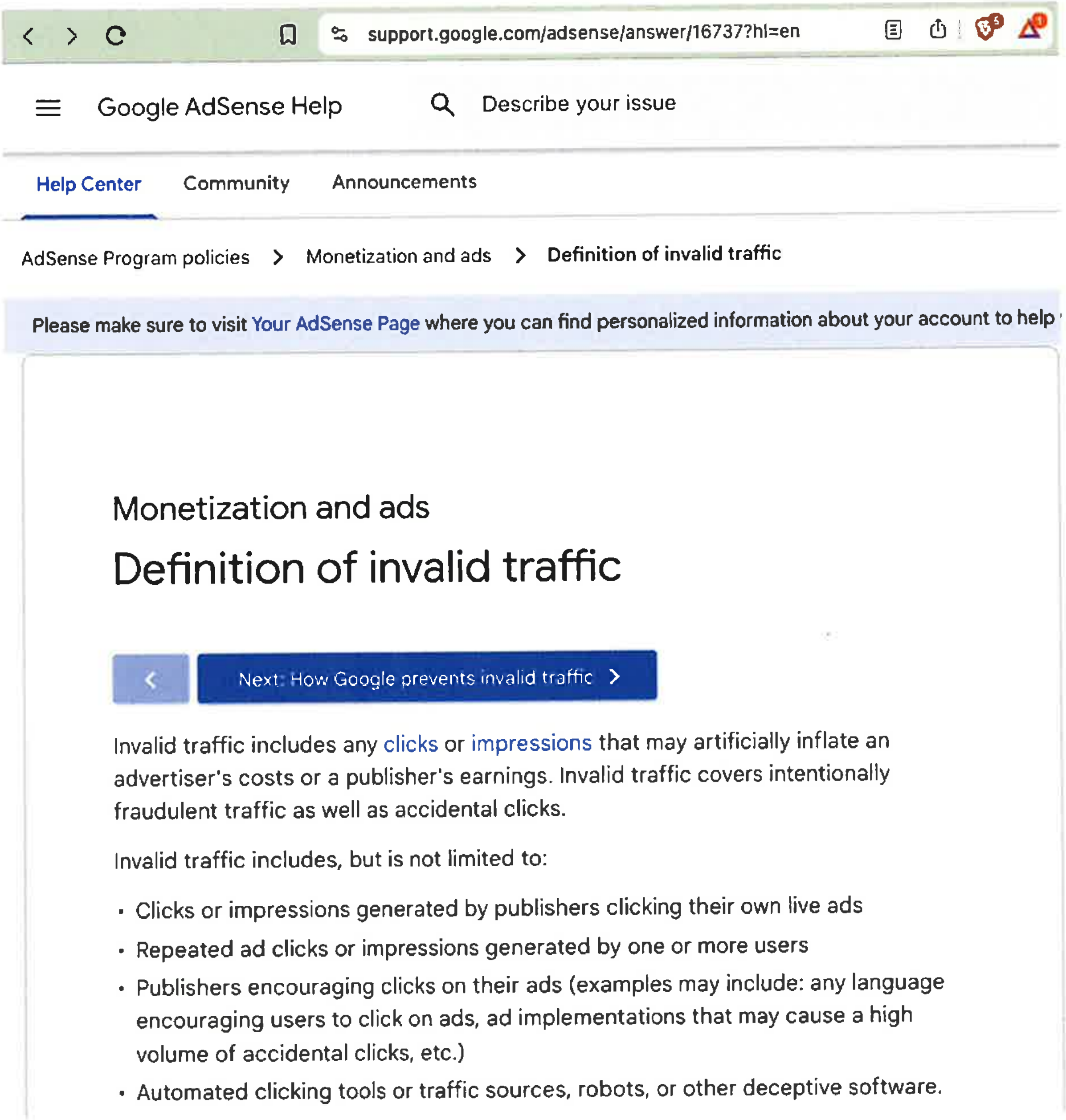
This addendum establishes two categories of IVT. The first, referred to herein as "General Invalid Traffic" or GIVT, consists of traffic identified through routine means of filtration executed through application of lists or with other standardized parameter checks. Key examples are:

- Known *invalid* data-center traffic *(determined to be a consistent source of invalid traffic; not including routing artifacts of legitimate users or virtual machine legitimate browsing)*;
- Bots and spiders or other crawlers[1] (except those as noted below in the "Sophisticated Invalid Traffic" category);
- Activity-based filtration using transaction-level data and parameters from campaign or application data;
- Non-browser user-agent headers or other forms of unknown browsers;

Screenshot of the MRC Invalid Traffic Detection and Filtration Standards Addendum - Categories of IVT and Associated General Requirements

According to Google, "Invalid traffic includes any clicks or impressions that may artificially inflate an advertiser's costs or a publisher's earnings. Invalid traffic covers intentionally fraudulent traffic as well as accidental clicks. Invalid traffic includes, but is not limited to: [...] Automated clicking tools or traffic sources, robots, or other deceptive software."

https://adalytics.io/blog/prebid-bot-filtration


support.google.com/adsense/answer/16737?hl=en
Google AdSense Help
Describe your issue
Help Center
Community
Announcements
AdSense Program policies > Monetization and ads > Definition of invalid traffic

Please make sure to visit Your AdSense Page where you can find personalized information about your account to help

Monetization and ads

Definition of invalid traffic

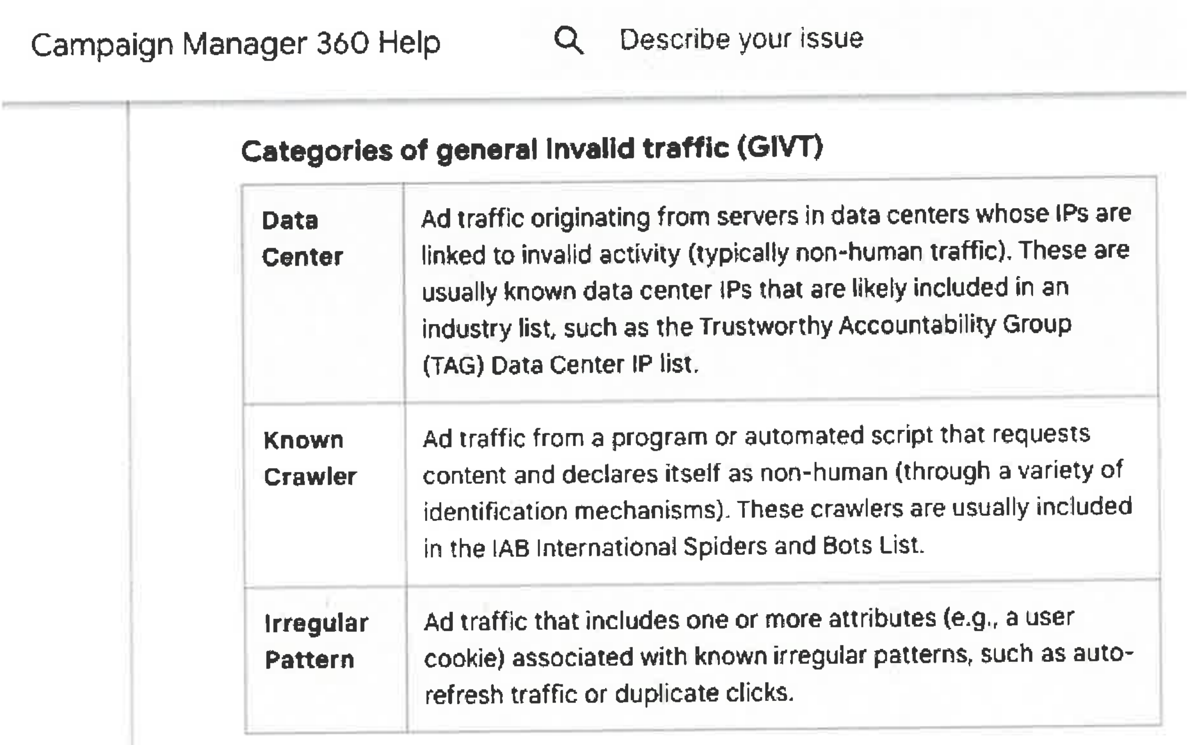
Next: How Google prevents invalid traffic >

Invalid traffic includes any clicks or impressions that may artificially inflate an advertiser's costs or a publisher's earnings. Invalid traffic covers intentionally fraudulent traffic as well as accidental clicks.

Invalid traffic includes, but is not limited to:

- Clicks or impressions generated by publishers clicking their own live ads
- Repeated ad clicks or impressions generated by one or more users
- Publishers encouraging clicks on their ads (examples may include: any language encouraging users to click on ads, ad implementations that may cause a high volume of accidental clicks, etc.)
- Automated clicking tools or traffic sources, robots, or other deceptive software.

Screenshot of Google AdSense Help - Definition of invalid traffic



Categories of general invalid traffic (GIVT)

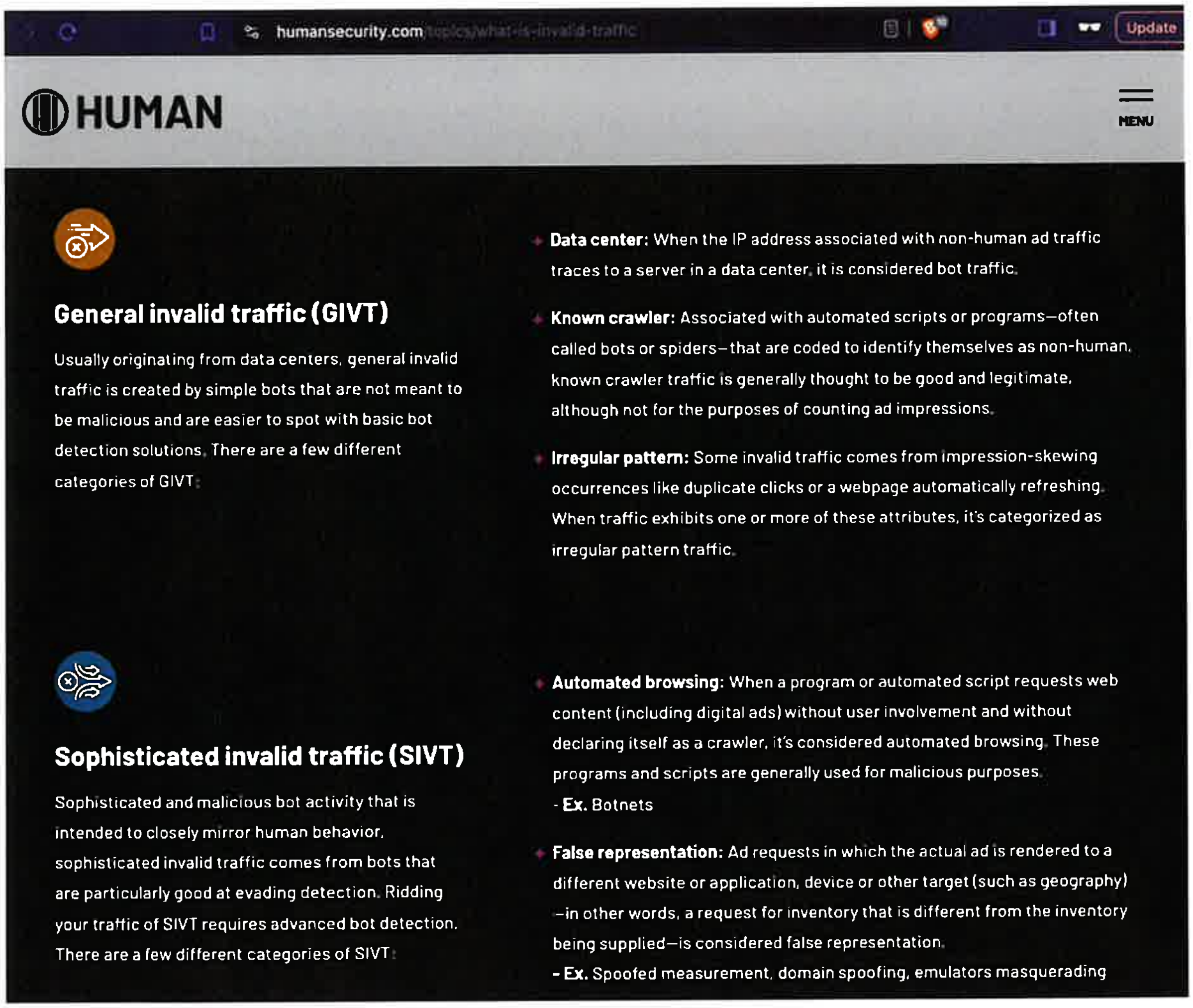
Data Center	Ad traffic originating from servers in data centers whose IPs are linked to invalid activity (typically non-human traffic). These are usually known data center IPs that are likely included in an industry list, such as the Trustworthy Accountability Group (TAG) Data Center IP list.
Known Crawler	Ad traffic from a program or automated script that requests content and declares itself as non-human (through a variety of identification mechanisms). These crawlers are usually included in the IAB International Spiders and Bots List.
Irregular Pattern	Ad traffic that includes one or more attributes (e.g., a user cookie) associated with known irregular patterns, such as auto-refresh traffic or duplicate clicks.

Source: Google Campaign Manager 360 Help - https://support.google.com/campaignmanager/answer/6076504?hl=en

According to HUMAN Security, an ad tech vendor, “Invalid Traffic (IVT) is generated when malicious bots view and click on ads in order to inflate conversion numbers, resulting in wasted advertiser spend.”

HUMAN Security defines General invalid traffic (GIVT) as “Usually originating from data centers, general invalid traffic is created by simple bots that are not meant to be malicious and are easier to spot with basic bot detection solutions. There are a few different categories of GIVT: Data center: When the IP address associated with non-human ad traffic traces to a server in a data center, it is considered bot traffic. Known crawler: Associated with automated scripts or programs—often called bots or spiders—that are coded to identify themselves as non-human, known crawler traffic is generally thought to be good and legitimate, although not for the purposes of counting ad impressions.”

HUMAN Security defines sophisticated invalid traffic (SIVT) as “Sophisticated and malicious bot activity that is intended to closely mirror human behavior, sophisticated invalid traffic comes from bots that are particularly good at evading detection. Ridding your traffic of SIVT requires advanced bot detection. There are a few different categories of SIVT: Automated browsing: When a program or automated script requests web content (including digital ads) without user involvement and without declaring itself as a crawler, it's considered automated browsing. These programs and scripts are generally used for malicious purposes. - Ex. Botnets"



General invalid traffic (GIVT)

Usually originating from data centers, general invalid traffic is created by simple bots that are not meant to be malicious and are easier to spot with basic bot detection solutions. There are a few different categories of GIVT:

- **Data center:** When the IP address associated with non-human ad traffic traces to a server in a data center, it is considered bot traffic.
- **Known crawler:** Associated with automated scripts or programs—often called bots or spiders—that are coded to identify themselves as non-human, known crawler traffic is generally thought to be good and legitimate, although not for the purposes of counting ad impressions.
- **Irregular pattern:** Some invalid traffic comes from impression-skewing occurrences like duplicate clicks or a webpage automatically refreshing. When traffic exhibits one or more of these attributes, it's categorized as irregular pattern traffic.

Sophisticated invalid traffic (SIVT)

Sophisticated and malicious bot activity that is intended to closely mirror human behavior, sophisticated invalid traffic comes from bots that are particularly good at evading detection. Ridding your traffic of SIVT requires advanced bot detection. There are a few different categories of SIVT:

- **Automated browsing:** When a program or automated script requests web content (including digital ads) without user involvement and without declaring itself as a crawler, it's considered automated browsing. These programs and scripts are generally used for malicious purposes.
  - **Ex.** Botnets
- **False representation:** Ad requests in which the actual ad is rendered to a different website or application, device or other target (such as geography) —in other words, a request for inventory that is different from the inventory being supplied—is considered false representation.
  - **Ex.** Spoofed measurement, domain spoofing, emulators masquerading

Screenshot of HUMAN Security's documentation on "What are the different types of invalid traffic?"

The Trade Desk defines General Invalid Traffic as: "Invalid traffic that can be identified through routine methods of filtration." The Trade Desk defines Sophisticated Invalid Traffic as: "A form of invalid traffic that requires advanced detection and analytics tools to identify."

Background - What is the IAB Tech Lab Spiders and Bots list ?

The User-Agent header is an HTTP header intended to identify the user agent responsible for making a given HTTP request. When a person browses the web via a browser on their phone rather than on the desktop, their phone's browser declares via the HTTP header that the user is browsing the web on a mobile browser (rather than a desktop browser).

A Chrome browser on Windows, a Firefox browser on Android, a Safari brower on iOS, and a Roku connected television device each have a distinct User-Agent header.

Similarly, when various "good" bots, such as GoogleBot or BingBot crawl the open internet, those bots openly declare themselves via the HTTP User-Agent header. If a website does not want to appear in Google or Bing search results, they can choose to block GoogleBot or Bingbot via their web hosting provider.

The Interactive Advertising Bureau (IAB) Tech Lab, an advertising industry trade group, and the Audit Bureau of Circulations (ABC) UK, a British trade group, create a reference list of known bots and spiders for ad tech vendors to use to detect and/or filter basic bot traffic.

According to the IAB Tech Lab, "*The IAB Tech Lab publishes a comprehensive list of such Spiders and Robots that helps companies identify automated traffic such as search engine crawlers, monitoring tools, and other non-human traffic that they don't want included in their analytics and billable counts [...] The IAB Tech Lab Spiders and Robots provides the industry two main purposes. First, the spiders and robots list consists of two text files: one for valid browsers or user agents and one for known robots. These lists are intended to be used together to comply with the "dual pass" approach to filtering as defined in the IAB's Ad Impression Measurement Guidelines (i.e., identify valid transactions using the valid browser list and then filter/remove invalid transactions using the known robots list). Second, the spiders and robots list supports the MRC's General Invalid Traffic Detection and Filtration Standard by* *providing a common industry resource and list for facilitating IVT detection and filtration."*

Section 7.1 of the IAB Tech Lab OpenRTB 2.x protocol specifies that ad exchanges and bidders should filter impressions from known bots who openly declare their user-agent. The IAB Tech Lab states:

Background: OpenRTB Protocol Guidance on ad bidding and serving to bots

The IAB Tech Lab is an advertising industry trade group which publishes the open real time bidding (OpenRTB) protocol which governs programmatic ad auctions that connect media publishers who sell ad spots to advertisers who wish to purchase and display ads.

The IAB Tech Lab OpenRTB protocol includes guidance on how ad exchanges and ad buying platforms should action bot traffic visiting websites and generating potential ad auction requests.

"An important issue in RTB is when impressions are triggered by software robots mimicking web browsers. Such robots may be implicitly or explicitly driving these false transactions. The following represents a set of symmetric best practices for exchanges and bidders to help recognize and reject these events.

Responsibility of the exchange - Make best effort to classify and reject non-human traffic (NHT) requests for ads to the exchange via the following best practices:

- *(Recommended) Filter impressions from known spiders via user-agent classification.*
- *(Recommended) Filter impressions from suspected NHT via a "detector".*

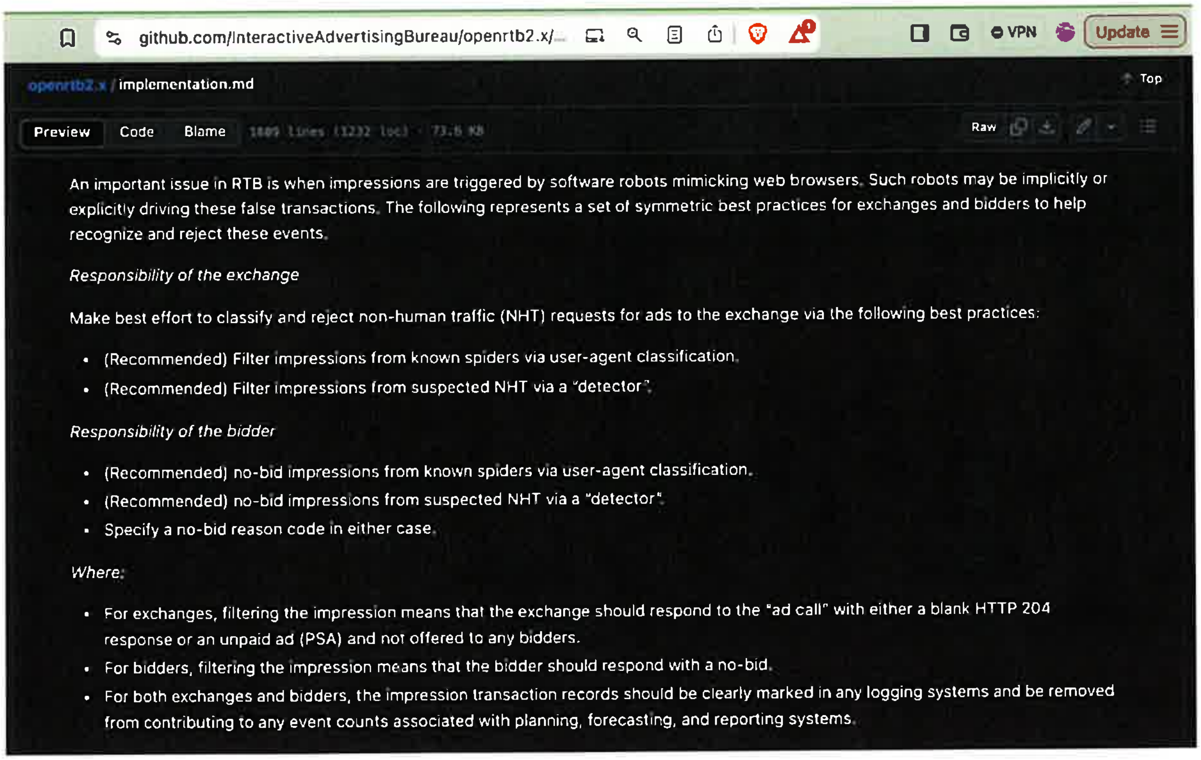
Responsibility of the bidder:

- *(Recommended) no-bid impressions from known spiders via user-agent classification.*
- *(Recommended) no-bid impressions from suspected NHT via a "detector".*

- *Specify a no-bid reason code in either case.*

Where:

- *For exchanges, filtering the impression means that the exchange should respond to the "ad call" with either a blank HTTP 204 response or an unpaid ad (PSA) and not offered to any bidders.*
- *For bidders, filtering the impression means that the bidder should respond with a no-bid.*
- *For both exchanges and bidders, the impression transaction records should be clearly marked in any logging systems and be removed from contributing to any event counts associated with planning, forecasting, and reporting systems."*


github.com/InteractiveAdvertisingBureau/openrtb2.x/...
VPN
Update
openrtb2.x / implementation.md
Top
Preview
Code
Blame
1889 Lines (1232 loc) · 73.6 KB
Raw

An important issue in RTB is when impressions are triggered by software robots mimicking web browsers. Such robots may be implicitly or explicitly driving these false transactions. The following represents a set of symmetric best practices for exchanges and bidders to help recognize and reject these events.

Responsibility of the exchange

Make best effort to classify and reject non-human traffic (NHT) requests for ads to the exchange via the following best practices:

- (Recommended) Filter impressions from known spiders via user-agent classification.
- (Recommended) Filter impressions from suspected NHT via a "detector".

Responsibility of the bidder

- (Recommended) no-bid impressions from known spiders via user-agent classification.
- (Recommended) no-bid impressions from suspected NHT via a "detector".
- Specify a no-bid reason code in either case.

Where:

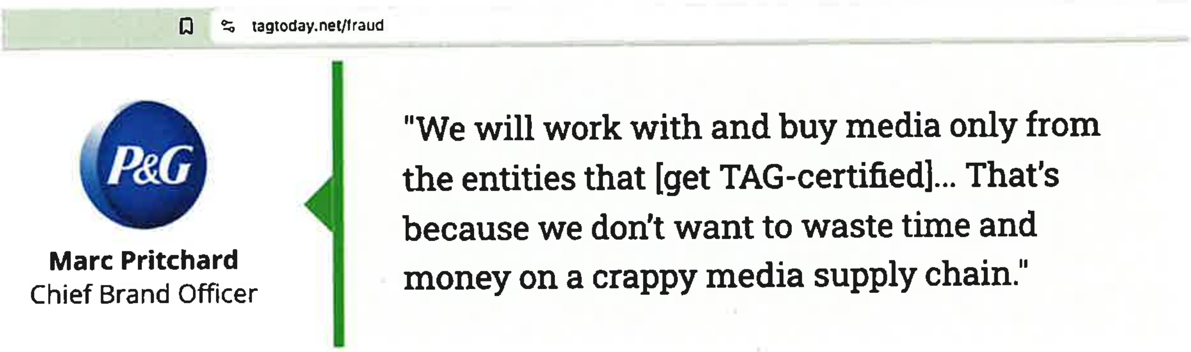
- For exchanges, filtering the impression means that the exchange should respond to the "ad call" with either a blank HTTP 204 response or an unpaid ad (PSA) and not offered to any bidders.
- For bidders, filtering the impression means that the bidder should respond with a no-bid.
- For both exchanges and bidders, the impression transaction records should be clearly marked in any logging systems and be removed from contributing to any event counts associated with planning, forecasting, and reporting systems.

Source: https://github.com/InteractiveAdvertisingBureau/openrtb2.x/blob/main/implementation.md#712---id-match-method-guidance-

Background - Trustworthy Accountability Group (TAG) - Certified Against Fraud

The Trustworthy Accountability Group (TAG) is a digital advertising initiative and trade group.

TAG launched its “Certified Against Fraud (CAF) Program in 2016 to combat invalid traffic in the digital advertising supply chain.”

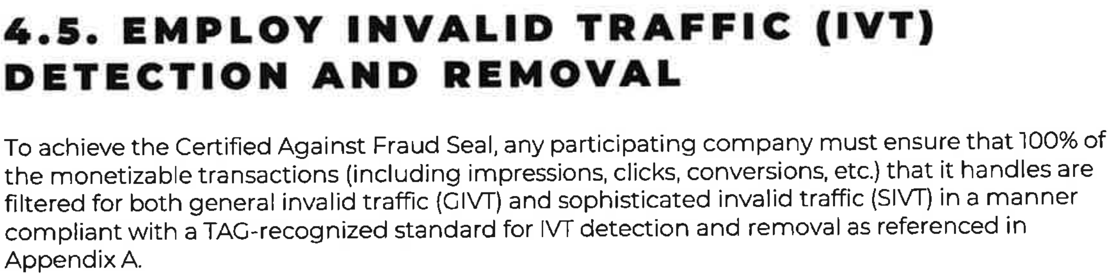


Marc Pritchard
Chief Brand Officer

"We will work with and buy media only from the entities that [get TAG-certified]... That's because we don't want to waste time and money on a crappy media supply chain."

Screenshot of a quote from P&G Chief Brand Officer Marc Pritchard on the TAG website

“To achieve the Certified Against Fraud Seal, any participating company must ensure that 100% of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are filtered for both general invalid traffic (GIVT) and sophisticated invalid traffic (SIVT) in a manner compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.”



4.5. EMPLOY INVALID TRAFFIC (IVT) DETECTION AND REMOVAL

To achieve the Certified Against Fraud Seal, any participating company must ensure that 100% of the monetizable transactions (including impressions, clicks, conversions, etc.) that it handles are filtered for both general invalid traffic (GIVT) and sophisticated invalid traffic (SIVT) in a manner compliant with a TAG-recognized standard for IVT detection and removal as referenced in Appendix A.

Source: TAG

“All inventory handled by a participating company – including inventory on that company’s

owned and operated media properties as well as any inventory handled by that company on

behalf of a third-party partner – must be filtered for GIVT and SIVT in a manner compliant with a

TAG-recognized standard for IVT detection and removal as referenced in Appendix A."

Background - Media Rating Council (MRC) - Invalid Traffic Detection and Filtration Standards Addendum

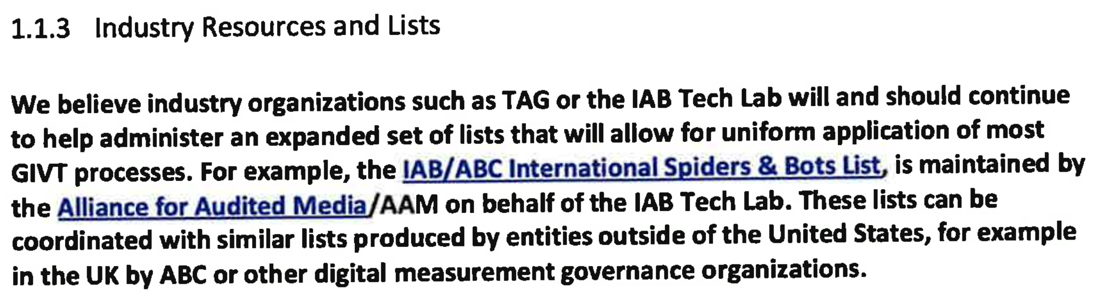
The Media Rating Council (MRC) is a US-based non profit organization that manages accreditations for media research and rating purposes. It performs accreditations for rating and research companies like Nielsen, comScore, and multiple digital measurement services. The MRC does not conduct the audit of the companies being accredited itself. The audits are done annually by accounting firms such as Ernst & Young. The company being accredited pays for the audit, with fees that could be in the hundreds of thousands or even millions of dollars.

The Media Rating Council has published Standards documents for "Invalid Traffic Detection and Filtration".

The document "presents additional Standards for the detection and filtration of invalid traffic applicable to all measurement organizations of advertising, content and related media metrics (including outcome measurement) subject to accreditation or certification audit. MRC's original guidance is contained in measurement guidelines maintained by the IAB."

The document explains, "Among the reasons why traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.)."

The MRC IVT Standards addendum discusses the role of IP address, user-agent, and industry reference lists in detecting invalid traffic (among many other topics and details).

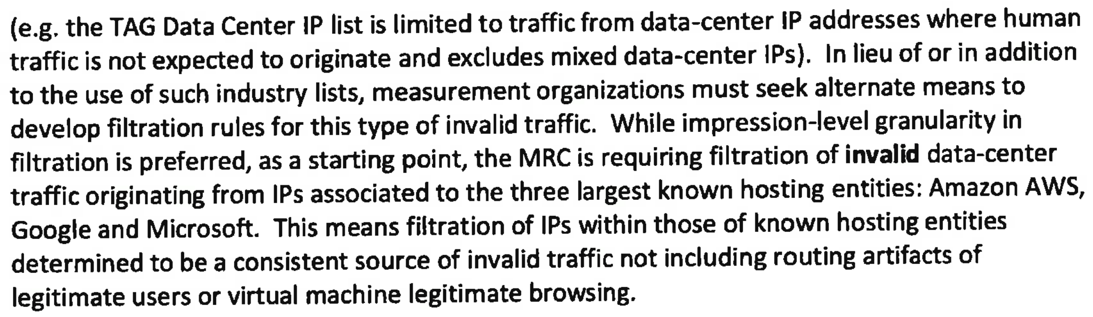


1.1.3 Industry Resources and Lists

We believe industry organizations such as TAG or the IAB Tech Lab will and should continue to help administer an expanded set of lists that will allow for uniform application of most GIVT processes. For example, the IAB/ABC International Spiders & Bots List, is maintained by the Alliance for Audited Media/AAM on behalf of the IAB Tech Lab. These lists can be coordinated with similar lists produced by entities outside of the United States, for example in the UK by ABC or other digital measurement governance organizations.

Source: Media Rating Council

The "*MRC is requiring filtration of invalid data-center traffic originating from IPs associated to the three largest known hosting entities: Amazon AWS, Google and Microsoft. This means filtration of IPs within those of known hosting entities determined to be a consistent source of invalid traffic not including routing artifacts of legitimate users or virtual machine legitimate browsing.*"



(e.g. the TAG Data Center IP list is limited to traffic from data-center IP addresses where human traffic is not expected to originate and excludes mixed data-center IPs). In lieu of or in addition to the use of such industry lists, measurement organizations must seek alternate means to develop filtration rules for this type of invalid traffic. While impression-level granularity in filtration is preferred, as a starting point, the MRC is requiring filtration of **invalid** data-center traffic originating from IPs associated to the three largest known hosting entities: Amazon AWS, Google and Microsoft. This means filtration of IPs within those of known hosting entities determined to be a consistent source of invalid traffic not including routing artifacts of legitimate users or virtual machine legitimate browsing.

Source: Media Rating Council

The Media Rating Council (MRC) states: "*The following techniques shall be employed by the measurement organization to the extent necessary to filter material General Invalid Transactions.*" The list includes a list of "parameter based detection", which includes "*non-Browser User-Agent Header" and "Known Invalid Data-Center Traffic"*.

Background - Media Rating Council (MRC) Accreditation for IVT Detection

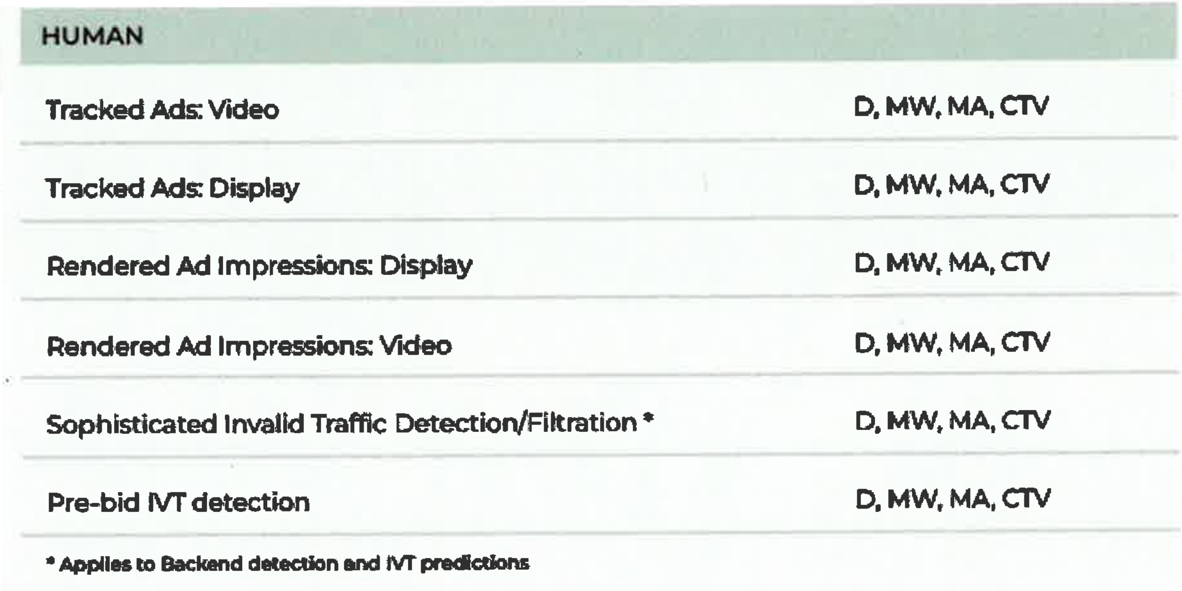
The Media Rating Council has provided accreditations to various vendors for invalid traffic detection and/or filtration.

One can visit the website of the Media Rating Council to see what accreditations various ad tech vendors have received from the MRC.

In 2021, HUMAN Security (f/k/a "White Ops) announced that it was the first company to "*Receive MRC Accreditation for Both Pre-Bid and Post-Bid Invalid Traffic Detection and Mitigation Across Desktop, Mobile Web, Mobile In-App and Connected TV*". The announcement states this "*includes the first-ever accreditation for pre-bid detection and mitigation of SIVT of its Advertising Integrity product (the solution formerly known as MediaGuard) across all platforms.*"

HUMAN's press release stated: "*White Ops today verifies more than ten trillion digital interactions per week, working directly with the largest internet platforms, DSPs and exchanges. With White Ops Advertising Integrity, platforms can tap into the most comprehensive pre-bid prevention and post-bid detection capabilities to verify the validity of advertising efforts across all channels. The White Ops bot mitigation platform uses a multilayered detection methodology to spot and stop sophisticated bots and fraud by using technical evidence, continuous adaptation, machine learning and threat intelligence. In most cases, White Ops delivers responses to partners in 10 milliseconds or less before a bid is made, saving time and money and ensuring that their advertising inventory can be trusted and fraud-free.*"

The MRC's website indicates that HUMAN Security (f/k/a "White Ops) has received MRC accreditations for "Pre-bid IVT detection" and "Sophisticated Invalid Traffic Detection/Filtration".



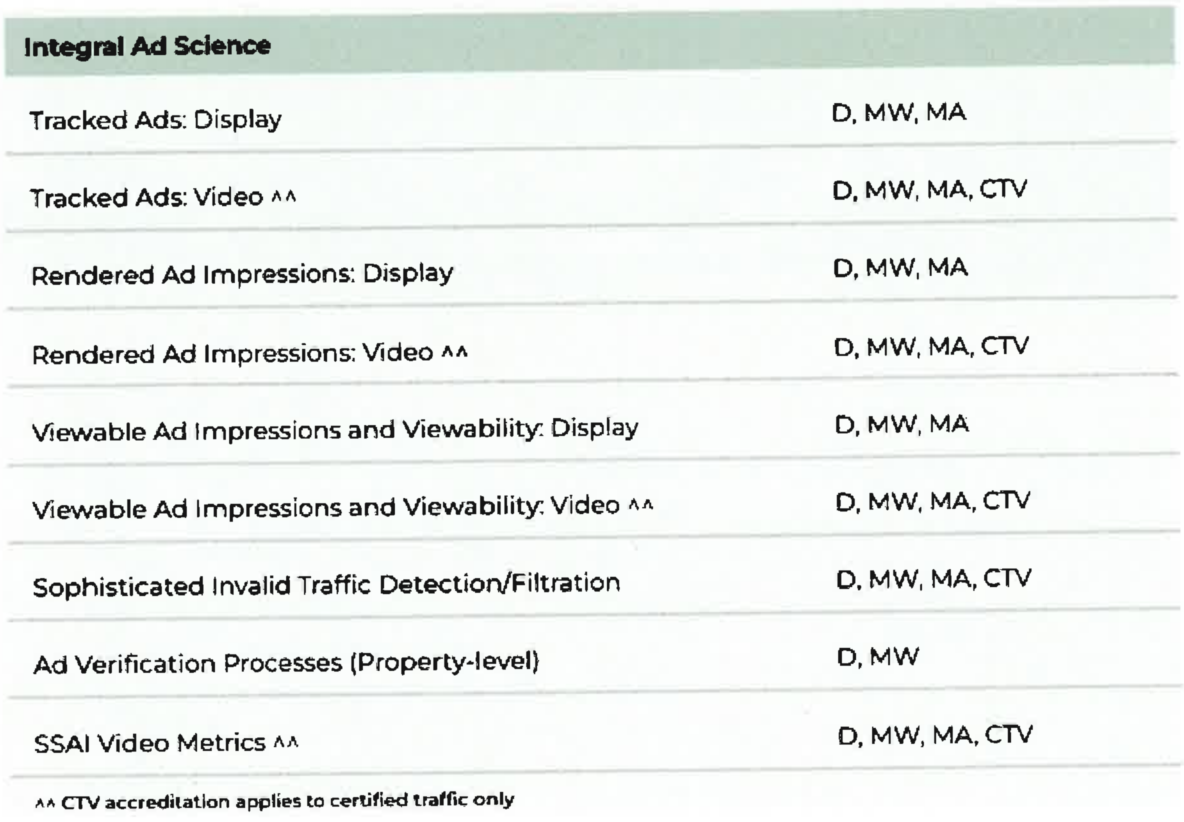
HUMAN	
Tracked Ads: Video	D, MW, MA, CTV
Tracked Ads: Display	D, MW, MA, CTV
Rendered Ad Impressions: Display	D, MW, MA, CTV
Rendered Ad Impressions: Video	D, MW, MA, CTV
Sophisticated Invalid Traffic Detection/Filtration *	D, MW, MA, CTV
Pre-bid IVT detection	D, MW, MA, CTV

* Applies to Backend detection and IVT predictions

Screenshot showing that HUMAN Security has received an accreditation from the Media Rating Council for “Sophisticated Invalid Traffic Detection/Filtration”. Source: Media Rating Council https://mediaratingcouncil.org/accreditation/digital

Other ad tech vendors that have received accreditations from the Media Rating Council include Integral Ad Science (IAS) and DoubleVerify.

In the screenshot below from the MRC’s website, one can see that IAS has received MRC accreditation for “Sophisticated Invalid Traffic Detection/Filtration”.



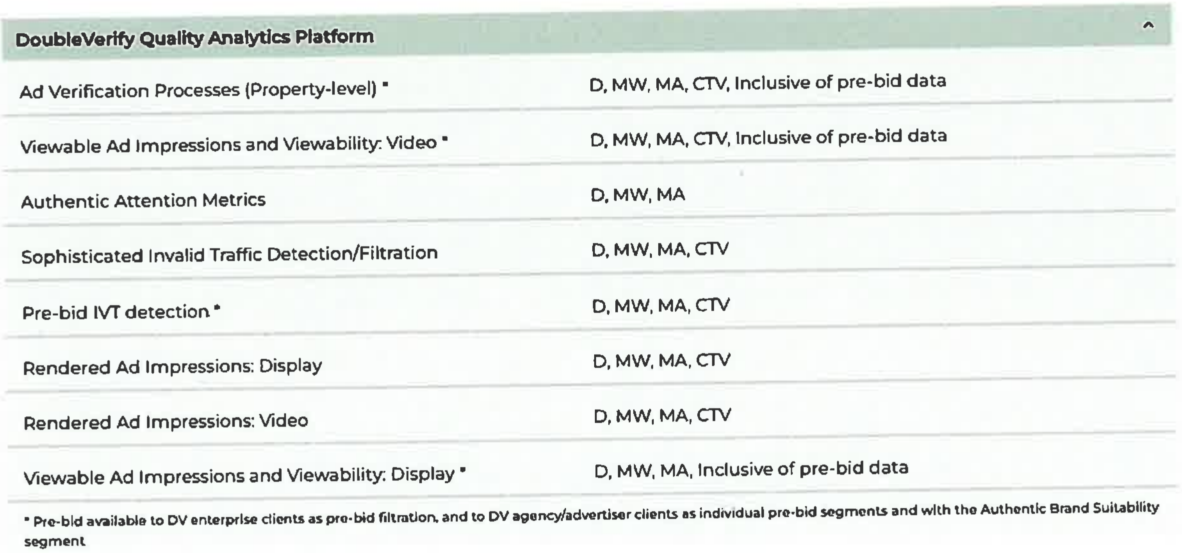
Integral Ad Science	
Tracked Ads: Display	D, MW, MA
Tracked Ads: Video ^^	D, MW, MA, CTV
Rendered Ad Impressions: Display	D, MW, MA
Rendered Ad Impressions: Video ^^	D, MW, MA, CTV
Viewable Ad Impressions and Viewability: Display	D, MW, MA
Viewable Ad Impressions and Viewability: Video ^^	D, MW, MA, CTV
Sophisticated Invalid Traffic Detection/Filtration	D, MW, MA, CTV
Ad Verification Processes (Property-level)	D, MW
SSAI Video Metrics ^^	D, MW, MA, CTV

^^ CTV accreditation applies to certified traffic only

Screenshot showing that Integral Ad Science (IAS) has received an accreditation from the Media Rating Council for "Sophisticated Invalid Traffic Detection/Filtration". Source: Media Rating Council https://mediaratingcouncil.org/accreditation/digital

The screenshot below shows that DoubleVerify has received MRC accreditation for "Pre-bid IVT detection" and "Sophisticated Invalid Traffic Detection/Filtration".

The Media Rating Council website explains that for DoubleVerify's "*Pre-bid IVT detection*", *"Pre-bid available to DV enterprise clients as pre-bid filtration, and to DV agency/advertiser clients as individual pre-bid segments and with the Authentic Brand Suitability segment"*.



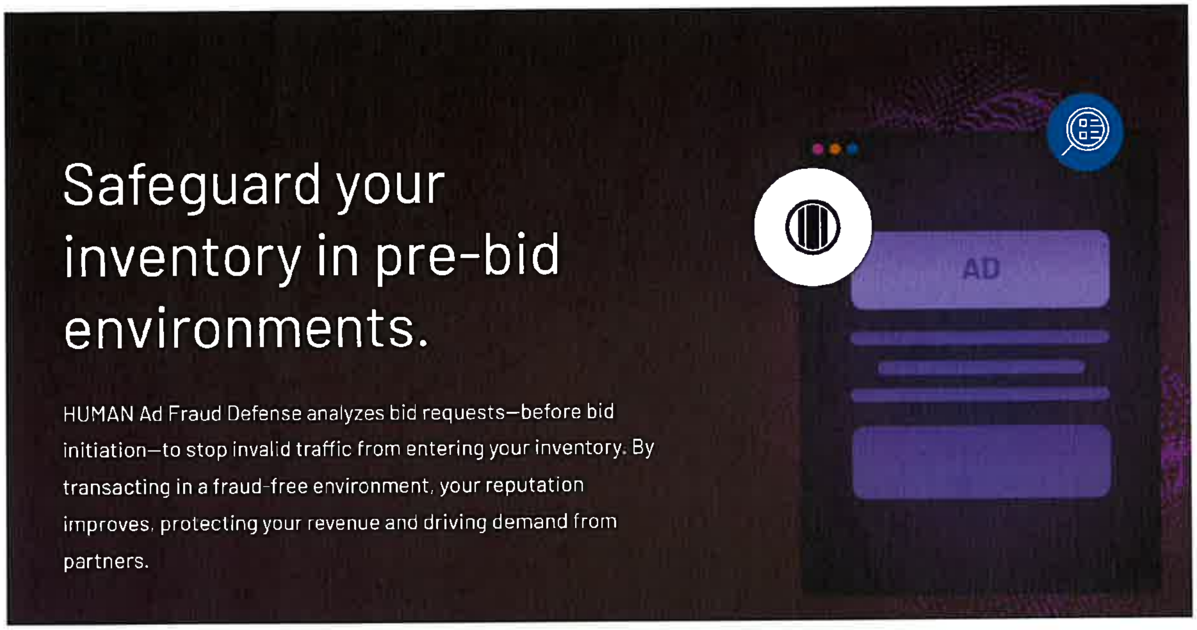
DoubleVerify Quality Analytics Platform	
Ad Verification Processes (Property-level) *	D, MW, MA, CTV, Inclusive of pre-bid data
Viewable Ad Impressions and Viewability: Video *	D, MW, MA, CTV, Inclusive of pre-bid data
Authentic Attention Metrics	D, MW, MA
Sophisticated Invalid Traffic Detection/Filtration	D, MW, MA, CTV
Pre-bid IVT detection *	D, MW, MA, CTV
Rendered Ad Impressions: Display	D, MW, MA, CTV
Rendered Ad Impressions: Video	D, MW, MA, CTV
Viewable Ad Impressions and Viewability: Display *	D, MW, MA, Inclusive of pre-bid data

* Pre-bid available to DV enterprise clients as pre-bid filtration, and to DV agency/advertiser clients as individual pre-bid segments and with the Authentic Brand Suitability segment

Screenshot showing that the DoubleVerify Quality Analytics Platform has received an accreditation from the Media Rating Council for "Sophisticated Invalid Traffic Detection/Filtration" and "Pre-bid IVT detection". Source: Media Rating Council https://mediaratingcouncil.org/accreditation/digital

Background - Ad tech vendors which partner with HUMAN Security

HUMAN Security's "Ad Fraud Defense" marketing page declares: *"Safeguard your inventory in pre-bid environments. HUMAN Ad Fraud Defense analyzes bid requests—before bid initiation—to stop invalid traffic from entering your inventory. By transacting in a fraud-free environment, your reputation improves, protecting your revenue and driving demand from partners."*

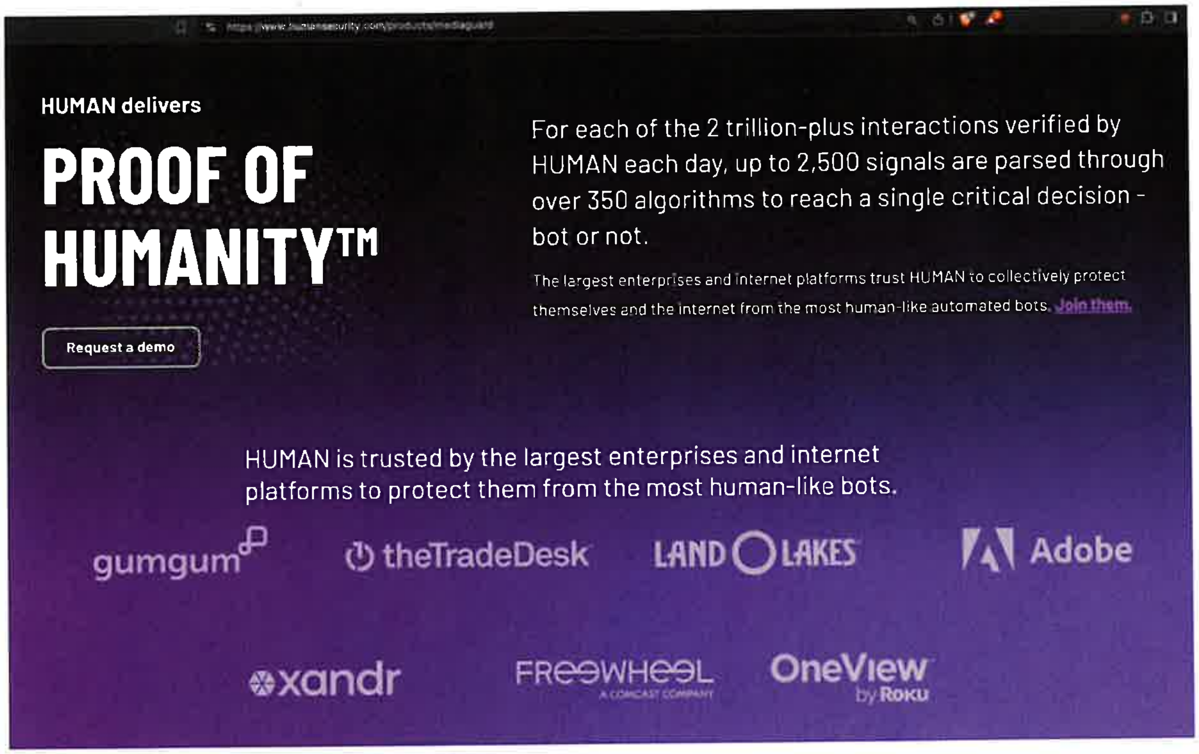


Safeguard your inventory in pre-bid environments.

HUMAN Ad Fraud Defense analyzes bid requests—before bid initiation—to stop invalid traffic from entering your inventory. By transacting in a fraud-free environment, your reputation improves, protecting your revenue and driving demand from partners.

Source: HUMAN Security

HUMAN Security's marketing page for its "MediaGuard" product states that "*For each of the 2 trillion-plus interactions verified by HUMAN each day, up to 2,500 signals are parsed through over 350 algorithms to reach a single critical decision - bot or not.*"


https://www.humansecurity.com/products/mediaguard
Request a demo
gumgum
theTradeDesk
LAND O LAKES
Adobe
xandr
FREEWHEEL A COMCAST COMPANY
OneView by Roku

HUMAN delivers

PROOF OF HUMANITY™

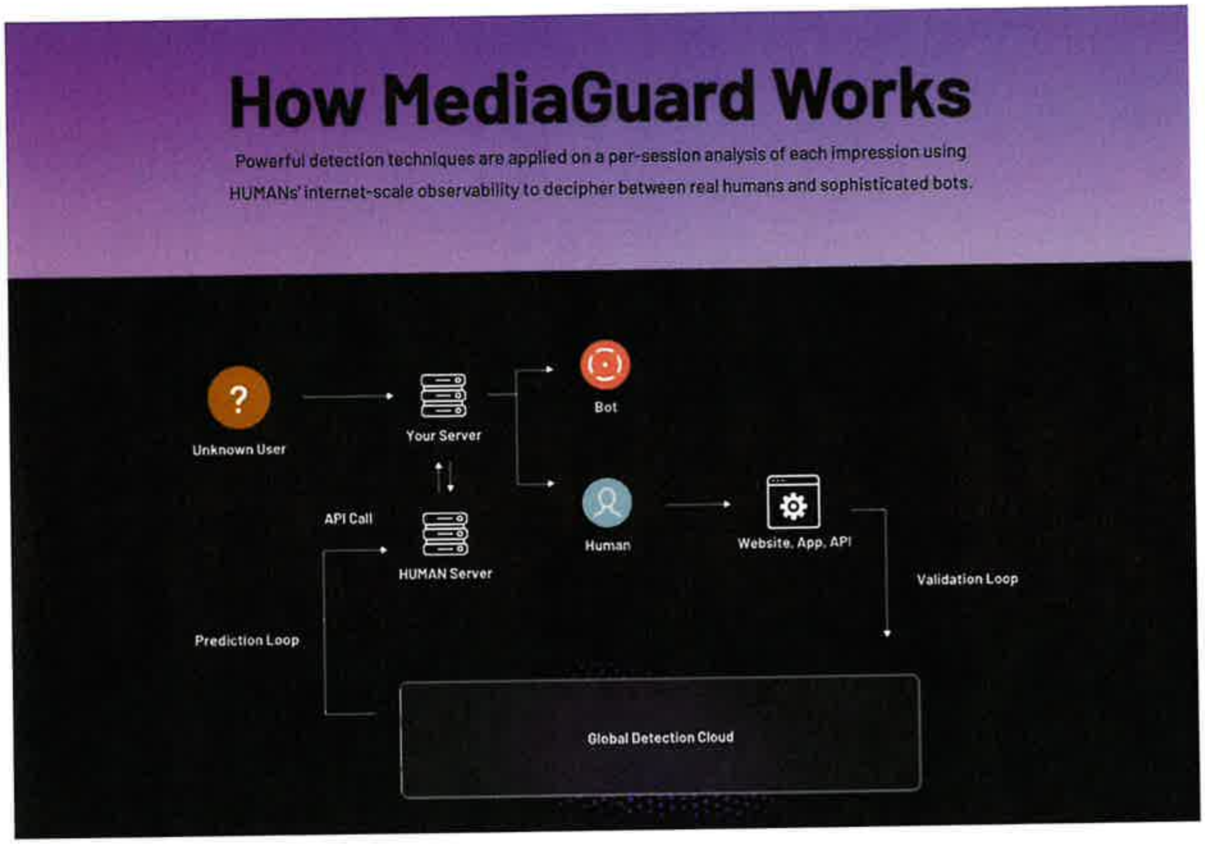
For each of the 2 trillion-plus interactions verified by HUMAN each day, up to 2,500 signals are parsed through over 350 algorithms to reach a single critical decision - bot or not.

The largest enterprises and internet platforms trust HUMAN to collectively protect themselves and the internet from the most human-like automated bots. Join them.

HUMAN is trusted by the largest enterprises and internet platforms to protect them from the most human-like bots.

Source: HUMAN Security

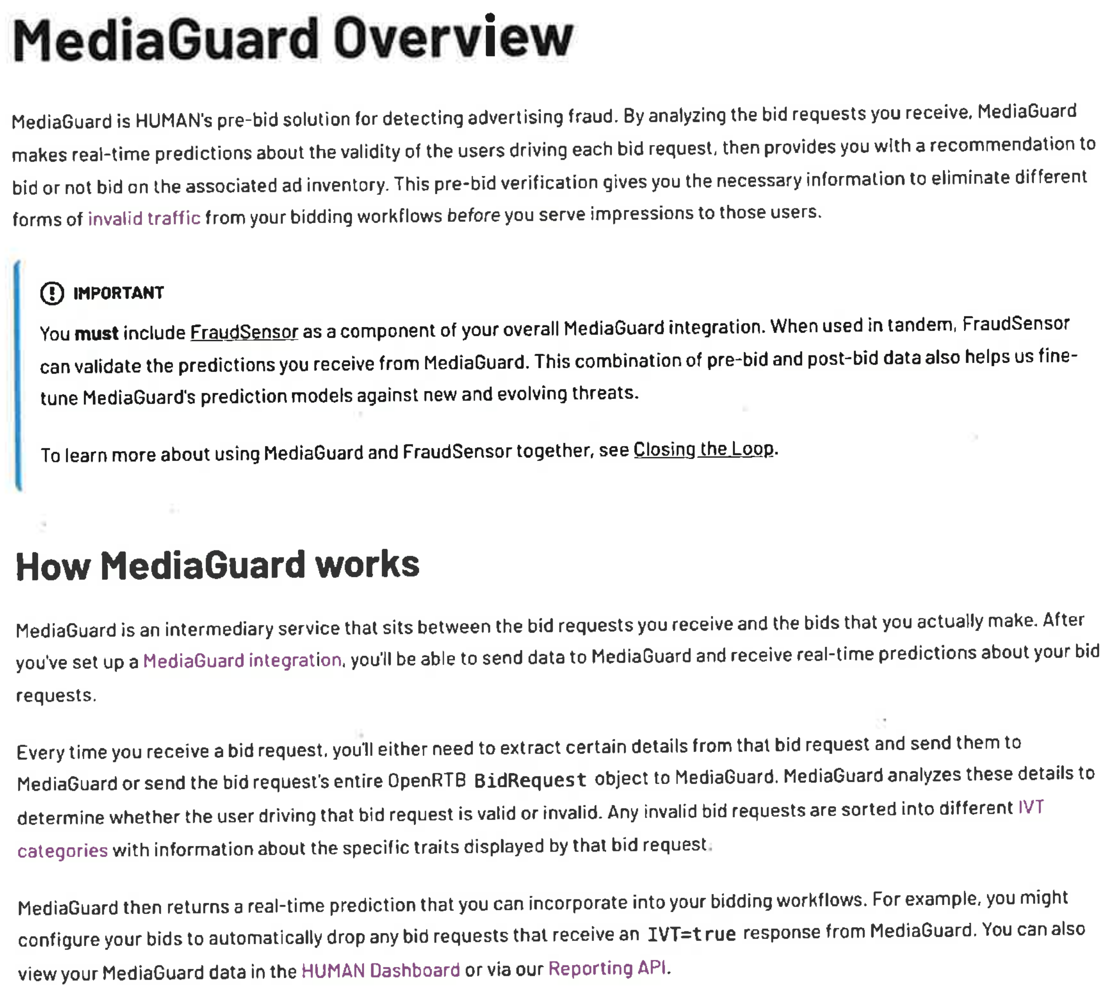
HUMAN Security's website explains that the way that MediaGuard works is through "*Powerful detection techniques are applied on a per-session analysis of each impression using HUMANs' internet-scale observability to decipher between real humans and sophisticated bots.*"


How MediaGuard Works
Powerful detection techniques are applied on a per-session analysis of each impression using HUMANs' internet-scale observability to decipher between real humans and sophisticated bots.
Unknown User
Your Server
Bot
Human
Website, App, API
API Call
HUMAN Server
Validation Loop
Prediction Loop
Global Detection Cloud

Source: HUMAN Security

HUMAN Security's public technical documentation states: "*MediaGuard is HUMAN's pre-bid solution for detecting advertising fraud. By analyzing the bid requests you receive, MediaGuard makes real-time predictions about the validity of the users driving each bid request, then provides you with a recommendation to bid or not bid on the associated ad inventory. This pre-bid verification gives you the necessary information to eliminate different forms of invalid traffic from your bidding workflows before you serve impressions to those users.*"

HUMAN further explains that "*MediaGuard is an intermediary service that sits between the bid requests you receive and the bids that you actually make. After you've set up a MediaGuard integration, you'll be able to send data to MediaGuard and receive real-time predictions about your bid requests. Every time you receive a bid request, you'll either need to extract certain details from that bid request and send them to MediaGuard or send the bid request's entire OpenRTB BidRequest object to MediaGuard. MediaGuard analyzes these details to determine whether* *the user driving that bid request is valid or invalid. Any invalid bid requests are sorted into different IVT categories with information about the specific traits displayed by that bid request. MediaGuard then returns a real-time prediction that you can incorporate into your bidding workflows. For example, you might configure your bids to automatically drop any bid requests that receive an IVT=true response from MediaGuard. You can also view your MediaGuard data in the HUMAN Dashboard or via our Reporting API."*



MediaGuard Overview

MediaGuard is HUMAN's pre-bid solution for detecting advertising fraud. By analyzing the bid requests you receive, MediaGuard makes real-time predictions about the validity of the users driving each bid request, then provides you with a recommendation to bid or not bid on the associated ad inventory. This pre-bid verification gives you the necessary information to eliminate different forms of invalid traffic from your bidding workflows *before* you serve impressions to those users.

> **IMPORTANT**
>
> You **must** include FraudSensor as a component of your overall MediaGuard integration. When used in tandem, FraudSensor can validate the predictions you receive from MediaGuard. This combination of pre-bid and post-bid data also helps us fine-tune MediaGuard's prediction models against new and evolving threats.
>
> To learn more about using MediaGuard and FraudSensor together, see Closing the Loop.

How MediaGuard works

MediaGuard is an intermediary service that sits between the bid requests you receive and the bids that you actually make. After you've set up a MediaGuard integration, you'll be able to send data to MediaGuard and receive real-time predictions about your bid requests.

Every time you receive a bid request, you'll either need to extract certain details from that bid request and send them to MediaGuard or send the bid request's entire OpenRTB `BidRequest` object to MediaGuard. MediaGuard analyzes these details to determine whether the user driving that bid request is valid or invalid. Any invalid bid requests are sorted into different IVT categories with information about the specific traits displayed by that bid request.

MediaGuard then returns a real-time prediction that you can incorporate into your bidding workflows. For example, you might configure your bids to automatically drop any bid requests that receive an `IVT=true` response from MediaGuard. You can also view your MediaGuard data in the HUMAN Dashboard or via our Reporting API.

Source: HUMAN Security Media Overview technical documentation

Many ad tech vendors have made public announcements about partnering with HUMAN Security (f/k/a "White Ops"), including using its MediaGuard product to check their ad inventory pre-bid.

For example, Index Exchange SSP stated in a press release:

"Index Exchange Partners with White Ops to Deliver Invalid Traffic Protection Against Sophisticated Bots Across All Global Inventory Channels"; "Index Exchange (IX), one of the world's largest independent ad exchanges, and White Ops, the global leader in collective protection against sophisticated bot attacks and fraud, today announced an expanded partnership that enhances Index Exchange's global inventory across all channels and regions. Through White Ops' comprehensive protection, the partnership protects the entirety of Index Exchange's global inventory. It allows buyers to purchase from IX's emerging channels, such as mobile app and Connected TV (CTV), with ***confidence that its supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible****"* (emphasis added).

Yieldmo SSP stated:

"White Ops, the global leader in bot mitigation, has announced a partnership with Yieldmo, one of the world's largest independent mobile ad marketplaces, to protect its programmatic demand partners from sophisticated bot attacks. [...] MediaGuard is a bot prevention API using machine-learning algorithms that learn and adapt in real-time to accurately block bot-driven ad requests before a buyer has the opportunity to bid on them. Eliminating fraudulent ad requests earlier in the bid process results in better overall performance for advertisers and yield for publishers. By leveraging White Ops' Bot Mitigation Platform, Yieldmo can accurately block sophisticated bots and pre-bid IVT without compromising the speed of their website and online operations. MediaGuard prevents bots and IVT across desktop, mobile web, mobile app, and connected TV (CTV) environments in real time before an impression is served."

Triplelift SSP stated in 2018:

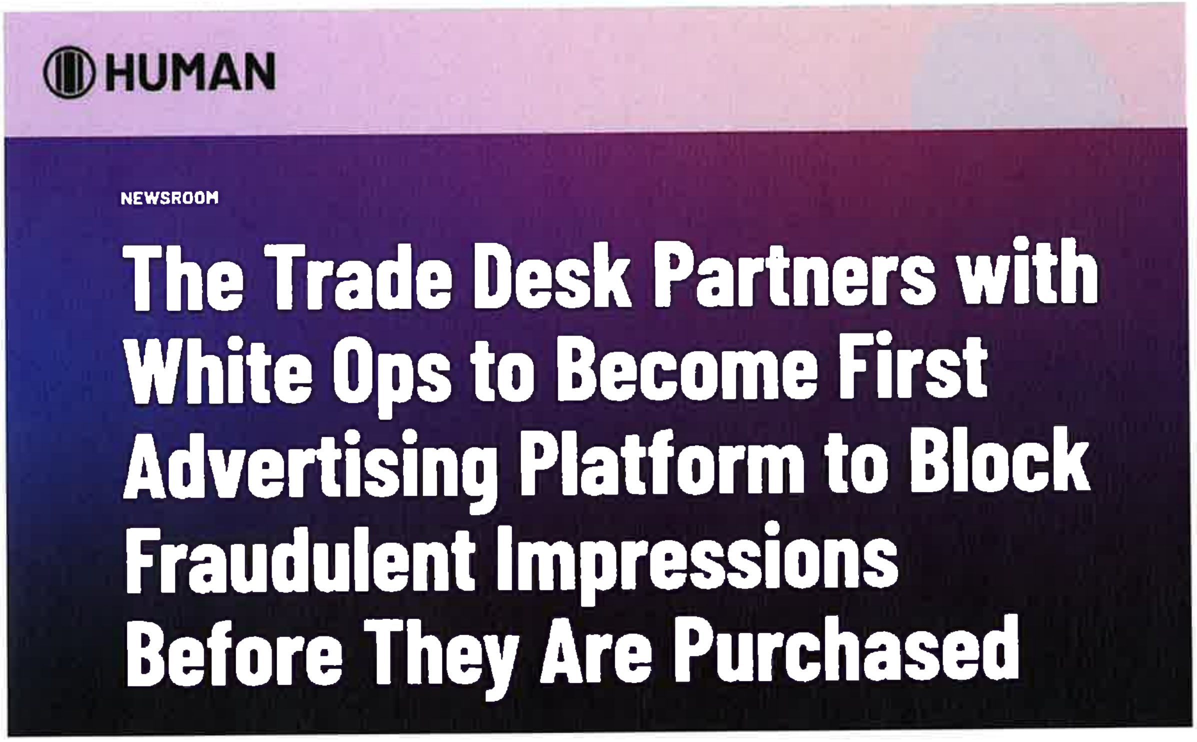
"Earlier this month our team announced that in partnership with White Ops, TripleLift would become the first native exchange to offer third-party verified pre-bid fraud prevention, across all of our inventory. This partnership allows TripleLift to leverage White Ops's MediaGuard, to assist in the pre-bid prevention of fraud across the entire exchange."

Pubmatic SSP stated:

"White Ops today announced its partnership with sell-side platform (SSP) PubMatic, to defend against fraudulent, non-human traffic impressions across PubMatic's video and mobile inventory. Through this partnership, PubMatic has globally implemented White Ops' pre-bid and post-bid solutions to provide ad fraud detection and prevention."

Demand side platform Trade Desk announced:

"White Ops and The Trade Desk [...] today announce a landmark deal that completely changes how the advertising industry tackles fraud. White Ops' Human Verification technology will aim to ensure that there is a ***human on the other end of every impression served on The Trade Desk*** *that runs through White Ops, in real time, protecting global advertisers and agencies from buying fraudulent impressions [...] For too long, invalid traffic has been part of our industry," said Jeff Green, CEO and co-founder of The Trade Desk. "There's no level of fraud that is acceptable. Our partnership with White Ops means that* ***we are the first advertising platform to block non-human impressions at the front door****. [...] As part of this initiative, White Ops and The Trade Desk will co-locate servers and data centers in North America, Europe and Asia, to* ***scan every biddable ad impression in real-time****. [...] When a non-human impression, known as "Sophisticated Invalid Traffic (SIVT)" within the advertising industry, is identified by White Ops, The Trade Desk will block that impression from serving. The intent is this technology will be* ***applied to every impression*** *The Trade Desk bids on that runs through White Ops, on a global basis. [...] Unlike other solutions, the goal here is to run all impressions across The Trade Desk's platform through White Ops, not just sampled impressions. Additionally, the Trade Desk has collaborated with the leading SSPs to bring a unified solution to market."* (emphasis added).

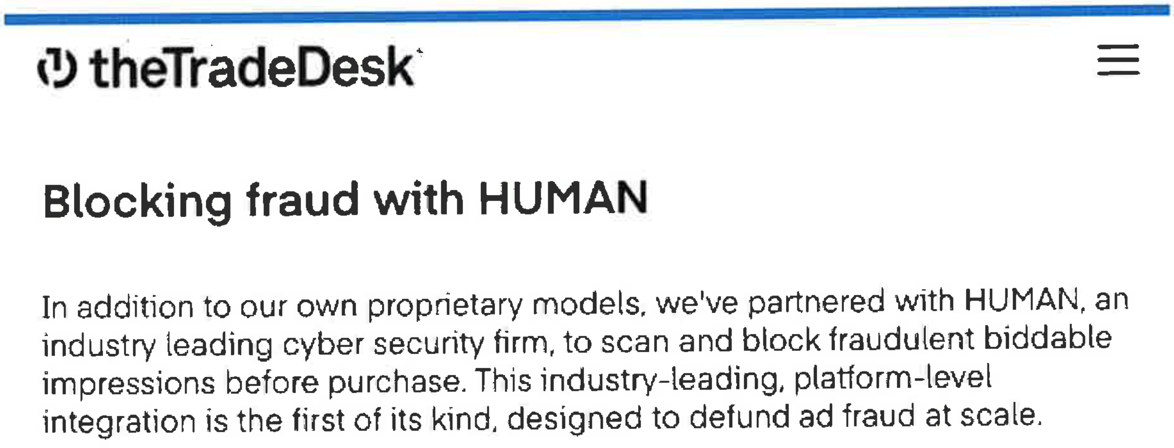


HUMAN

NEWSROOM

The Trade Desk Partners with White Ops to Become First Advertising Platform to Block Fraudulent Impressions Before They Are Purchased

Screenshot of HUMAN Security's website, showing a press release from 2017



theTradeDesk

Blocking fraud with HUMAN

In addition to our own proprietary models, we've partnered with HUMAN, an industry leading cyber security firm, to scan and block fraudulent biddable impressions before purchase. This industry-leading, platform-level integration is the first of its kind, designed to defund ad fraud at scale.

Screenshot of Trade Desk's website, showing the firm partners with HUMAN Security

AD TECH INDUSTRY NEWS

The Trade Desk and White Ops Are Teaming Up to Block Bot Traffic Before Advertisers Buy It

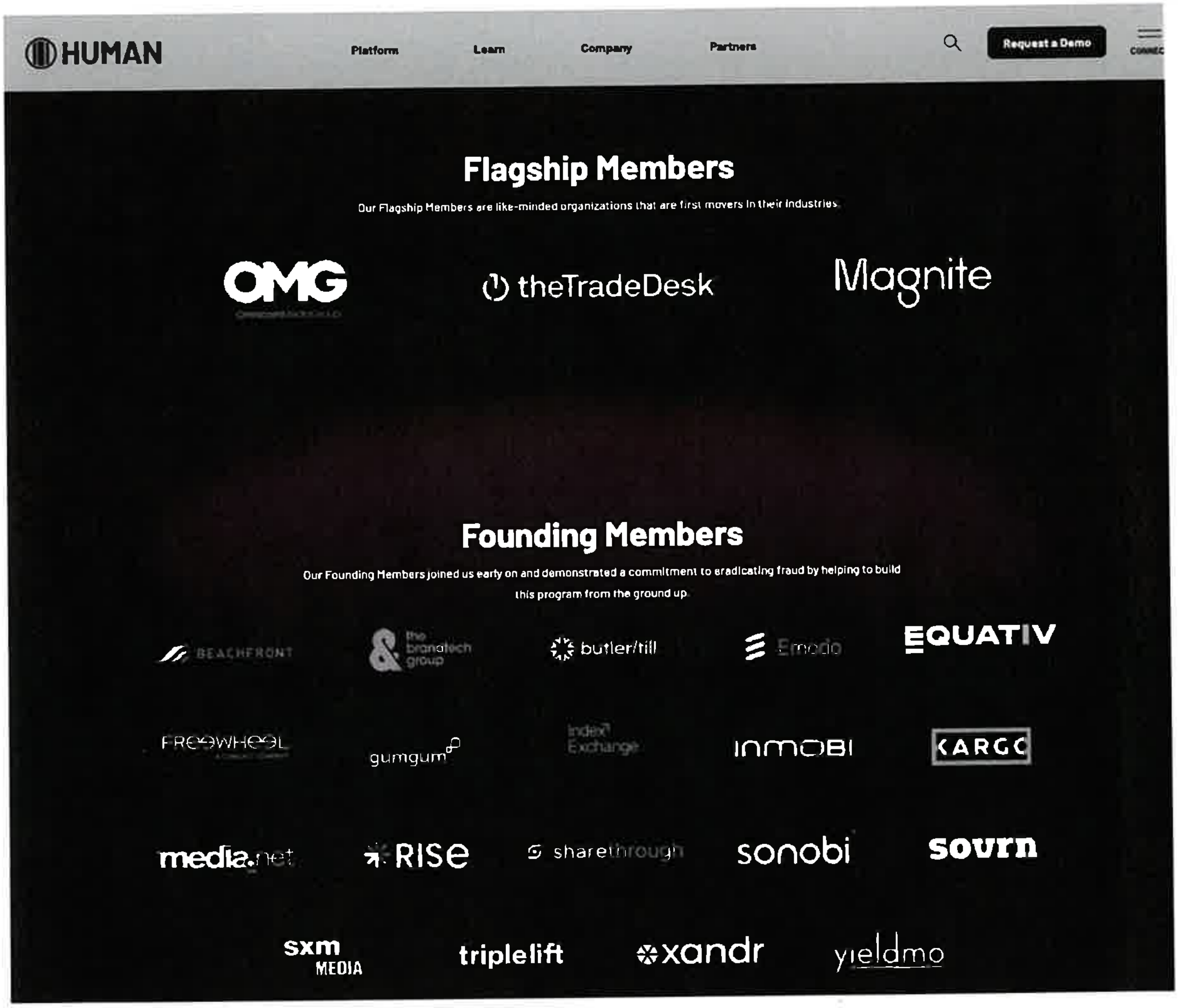
The companies think it's 'a game-changer'

https://www.adweek.com/performance-marketing/the-trade-desk-and-white-ops-are-teaming-up-to-block-bot-traffic-before-advertisers-buy-it/

Xandr (f/k/a AppNexus) and now owned by Microsoft, announced:

*"Xandr [...] and HUMAN, a cybersecurity company best known for collectively protecting enterprises from bot attacks, today announced an **expansion to HUMAN's existing pre-bid bot protection** within the Xandr platform, to provide an additional layer of protection against fraud and sophisticated bot attacks as emerging formats like connected TV (CTV) scale in availability and demand. This integration connects the full breadth of HUMAN's Advertising Integrity suite of ad fraud detection and prevention solutions to Xandr's buy-and sell-side platforms [...] Xandr protects its platform **before a bid is even made**—including within CTV—to continue delivering success to its publishers and advertisers. HUMAN recently became the first company to receive accreditation from the Media Rating Council (MRC) for pre and post-bid protection against Sophisticated Invalid Traffic (SIVT) for desktop, mobile web, mobile in-app, and CTV."*

Many ad tech vendors are part of the HUMAN Security's "Human Collective."



Flagship Members

Our Flagship Members are like-minded organizations that are first movers in their industries.

Founding Members

Our Founding Members joined us early on and demonstrated a commitment to eradicating fraud by helping to build this program from the ground up.

List of Flagship and Founding Members of HUMAN Security's "Human Collective". Source: https://www.humansecurity.com/company/the-human-collective. Participation in the Human Collective entails: "Technology - Powered by HUMAN's proprietary technology and Modern Defense Platform, we can ensure members are protecting themselves and each other."

A list of vendors who issued public statements or claimed to have partnered with HUMAN Security (f/k/a "White Ops") can be seen below.

The Trade Desk	https://www.humansecurity.com/newsroom/the-trade-desk-partners-with-white-ops-to-become-first-advertising-platform-to-block-fraudulent-impressions-before-they-are-purchased	8/31/2017

https://adalytics.io/blog/prebid-bot-filtration

Microsoft Xandr	https://www.prnewswire.com/news-releases/appnexus-expands-inventory-quality-initiative-through-partnership-with-white-ops-300666958.html	6/15/2018
Index Exchange	https://www.humansecurity.com/newsroom/index-exchange-partners-with-white-ops	8/12/2020
Google	https://support.google.com/campaignmanager/answer/6076504?hl=en	N/A
Sovrn	https://www.humansecurity.com/newsroom/the-human-collective-grows-more-than-5x-since-april-launch	10/13/2021
Yieldmo	https://www.humansecurity.com/learn/blog/yieldmo-and-white-ops-ensuring-squeaky-clean-mobile-inventory	9/10/2019
Sharethrough	https://www.sharethrough.com/blog/sharethrough-founding-member-of-the-human-collective-in-effort-to-keep-ads-human	10/27/2021
Kargo	https://www.humansecurity.com/newsroom/kargos-curated-marketplace-boasts-less-than-0.3-of-invalid-traffic-following-implementation-of-white-ops-mediaguard	5/29/2019
Gumgum	https://www.businesswire.com/news/home/20190529005284/en/GumGum-Partners-with-White-Ops-to-Deliver-Comprehensively-Safe-Ad-Exchange	5/29/2019
Triplelift	https://www.humansecurity.com/newsroom/triplelift-and-white-ops-partner-to-fight-fraud-in-native-advertising	5/1/2018
Magnite	https://www.businesswire.com/news/home/20161220005758/en/Joint-Statement-From-White-Ops-CEO-and-Rubicon-Project-President-on-Successful-Efforts-Countering-Russian-Ad-Fraud	12/20/2016
Pubmatic	https://www.humansecurity.com/newsroom/pubmatic-partners-with-white-ops-to-fight-bot-fraud-and-drive-higher-transparency-in-video-inventory	12/5/2017
Sonobi	https://www.prnewswire.com/news-releases/sonobi-partners-with-human-formerly-white-ops-to-safeguard-platform-from-sophisticated-bot-fraud-301286928.html	5/11/2021
Freewheel	https://www.humansecurity.com/newsroom/freewheel-and-white-ops-expand-partnership-globally-to-further-deepen-trust-in-premium-video-inventory	4/29/2020
Media.net	https://www.humansecurity.com/newsroom/white-ops-media.net-partnership-extends-pre-bid-fraud-protection-for-brands	5/15/2019
Beachfront	https://www.humansecurity.com/newsroom/white-ops-beachfront	5/15/2018
Primis	https://www.humansecurity.com/newsroom/primis-expands-partnership-with-white-ops-in-fight-against-fraud-to-create-a-clean-and-trusted-video-supply-chain	9/1/2020
Omnicom	https://www.humansecurity.com/newsroom/human-formerly-white-ops-launches-the-human-collective-to-protect-against-bot-attacks-and-fraud-across-advertising-supply-chain	4/14/2021

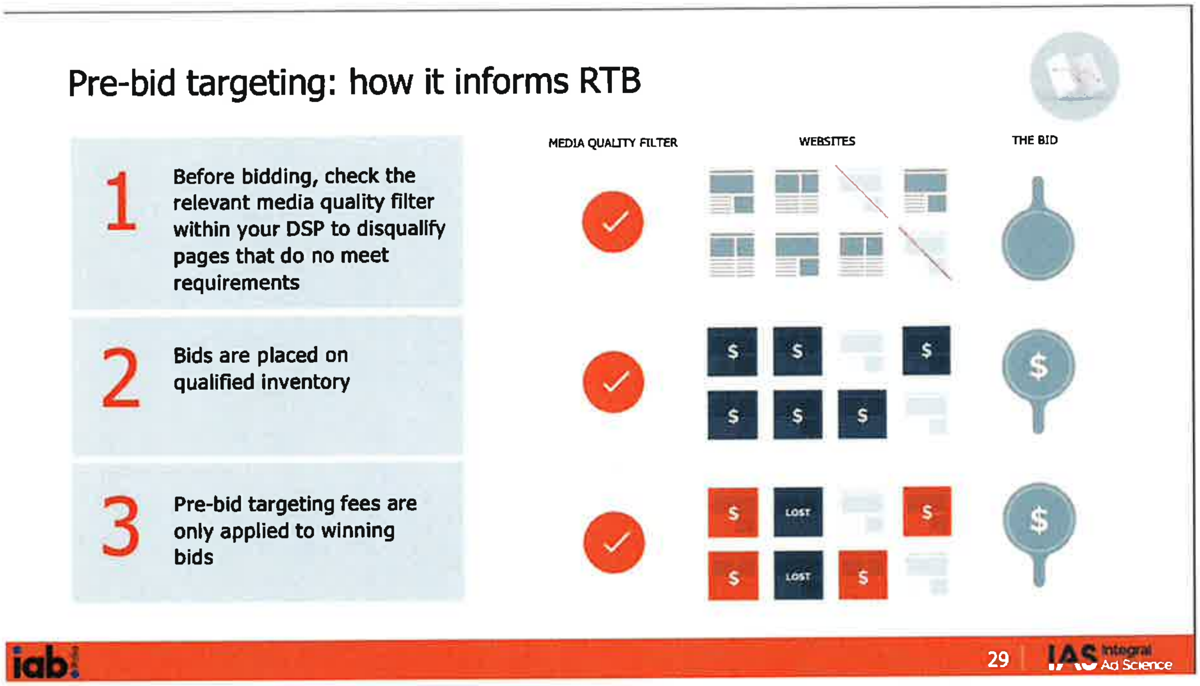
Background - What is “Pre-bid targeting” in digital advertising?

In programmatic digital advertising, “Real Time Bidding” (RTB or OpenRTB) is a protocol that governs digital ad auctions, where publishers and advertisers can offer to sell and buy ad placements (respectively).

Before an advertiser “bids” on a given programmatic ad auction, “pre-bid” data segments and solutions can inform the ad bidding process.

For example, according to the IAB and Integral Ad Science (IAS), an ad verification vendor, the way “Pre-bid targeting” informs real time bidding is as follows:

1. “Before bidding, check the relevant media quality filter within your DSP to disqualify pages that do not meet requirements”
2. “Bids are placed on qualified inventory”
3. “Pre-bid targeting fees are only applied to winning bids”



Pre-bid targeting: how it informs RTB

1 Before bidding, check the relevant media quality filter within your DSP to disqualify pages that do no meet requirements

2 Bids are placed on qualified inventory

3 Pre-bid targeting fees are only applied to winning bids

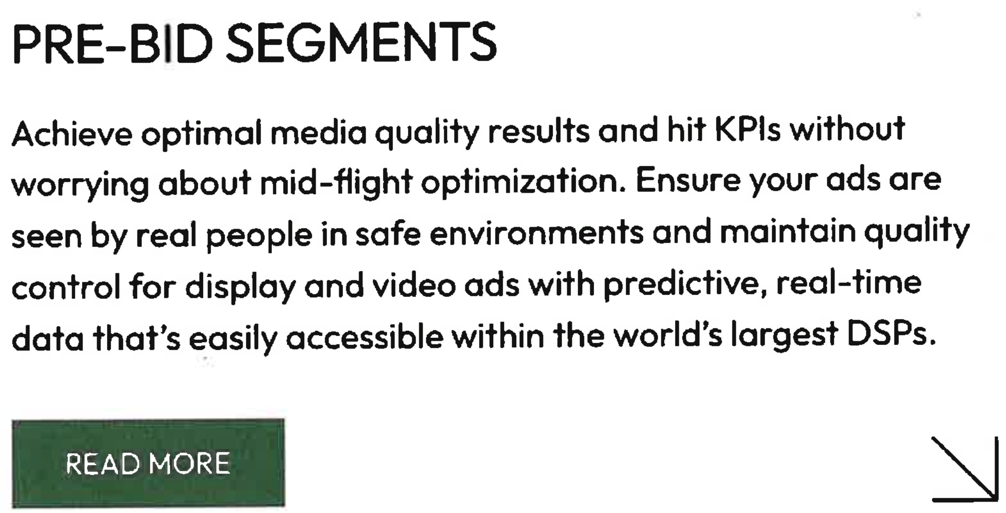
Source: IAB and IAS

Background - Integral Ad Science (IAS) ad fraud solutions

Integral Ad Science (IAS) is an ad verification company that has received multiple Media Rating Council accreditations, and is TAG "Certified Against Fraud".

IAS provides ad verification solutions to both advertisers and to media publishers.

IAS offers "pre-bid" targeting data solutions in various ad buying platforms (known as "demand side platforms" or DSPs), such as Trade Desk, Beeswax, and Google DV360.

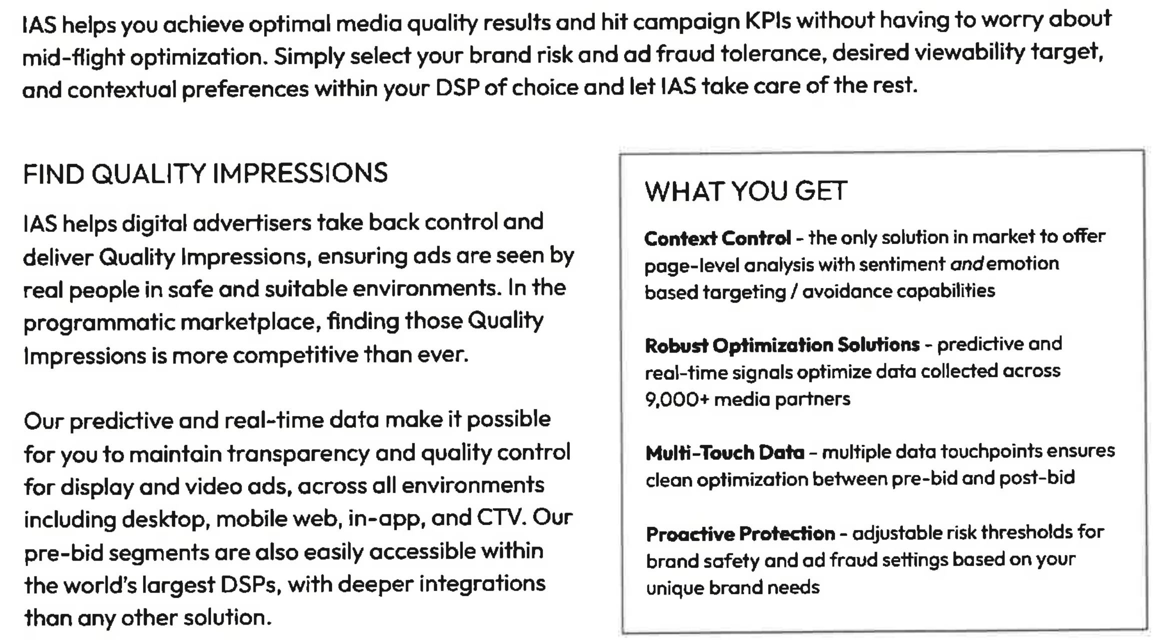


PRE-BID SEGMENTS

Achieve optimal media quality results and hit KPIs without worrying about mid-flight optimization. Ensure your ads are seen by real people in safe environments and maintain quality control for display and video ads with predictive, real-time data that's easily accessible within the world's largest DSPs.

Source: IAS

IAS's website states that "utilizing IAS pre-bid segments" can help advertisers "Only bid on quality Inventory" in programmatic ad auctions.



IAS helps you achieve optimal media quality results and hit campaign KPIs without having to worry about mid-flight optimization. Simply select your brand risk and ad fraud tolerance, desired viewability target, and contextual preferences within your DSP of choice and let IAS take care of the rest.

FIND QUALITY IMPRESSIONS

IAS helps digital advertisers take back control and deliver Quality Impressions, ensuring ads are seen by real people in safe and suitable environments. In the programmatic marketplace, finding those Quality Impressions is more competitive than ever.

Our predictive and real-time data make it possible for you to maintain transparency and quality control for display and video ads, across all environments including desktop, mobile web, in-app, and CTV. Our pre-bid segments are also easily accessible within the world's largest DSPs, with deeper integrations than any other solution.

WHAT YOU GET

Context Control - the only solution in market to offer page-level analysis with sentiment *and* emotion based targeting / avoidance capabilities

Robust Optimization Solutions - predictive and real-time signals optimize data collected across 9,000+ media partners

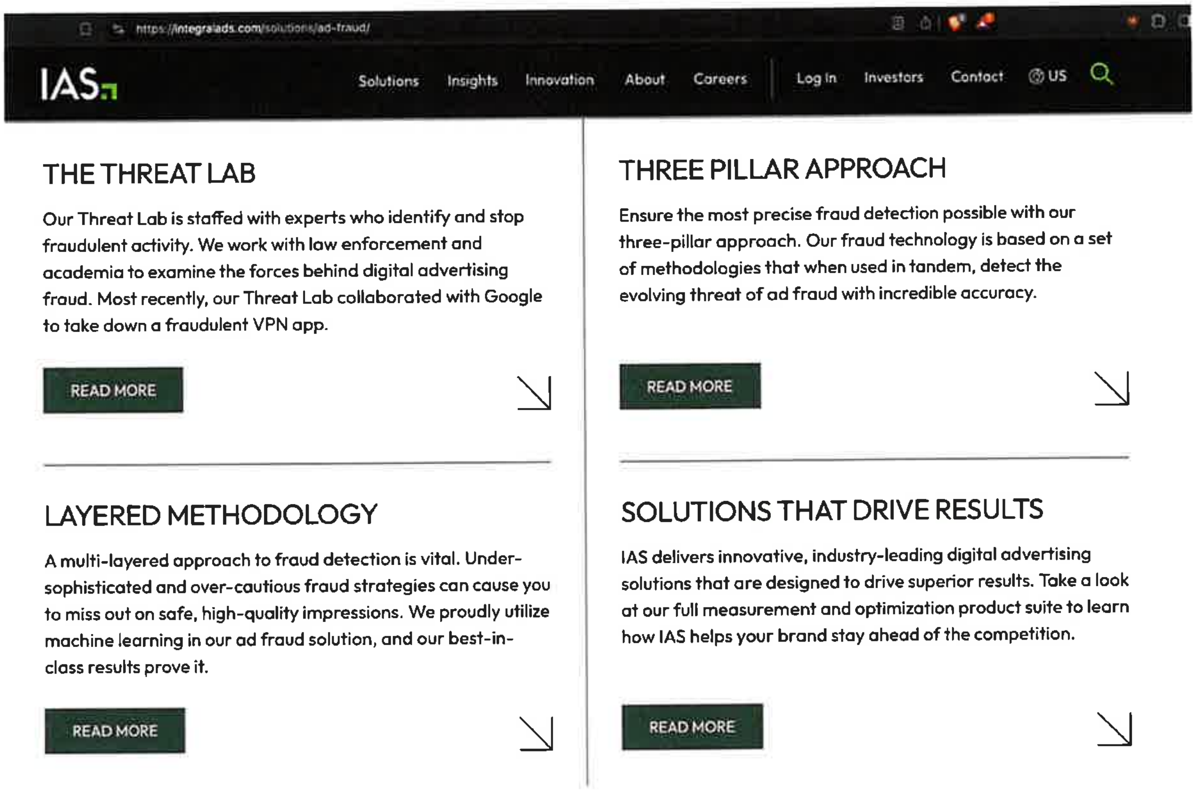
Multi-Touch Data - multiple data touchpoints ensures clean optimization between pre-bid and post-bid

Proactive Protection - adjustable risk thresholds for brand safety and ad fraud settings based on your unique brand needs

Source: IAS

IAS's website states: "*IAS is a leader in the fight against ad fraud through a balanced approach and ongoing research. Our team of specialized analysts, engineers, white-hat-hackers, and data scientists is taking on invalid traffic from every angle to create the most advanced solutions in the market [...] Ensure the most precise fraud detection possible with our three-pillar approach. Our fraud technology is based on a set of methodologies that when used in tandem, detect the evolving threat of ad fraud with incredible accuracy.*"

https://adalytics.io/blog/prebid-bot-filtration



THE THREAT LAB

Our Threat Lab is staffed with experts who identify and stop fraudulent activity. We work with law enforcement and academia to examine the forces behind digital advertising fraud. Most recently, our Threat Lab collaborated with Google to take down a fraudulent VPN app.

READ MORE

THREE PILLAR APPROACH

Ensure the most precise fraud detection possible with our three-pillar approach. Our fraud technology is based on a set of methodologies that when used in tandem, detect the evolving threat of ad fraud with incredible accuracy.

READ MORE

LAYERED METHODOLOGY

A multi-layered approach to fraud detection is vital. Under-sophisticated and over-cautious fraud strategies can cause you to miss out on safe, high-quality impressions. We proudly utilize machine learning in our ad fraud solution, and our best-in-class results prove it.

READ MORE

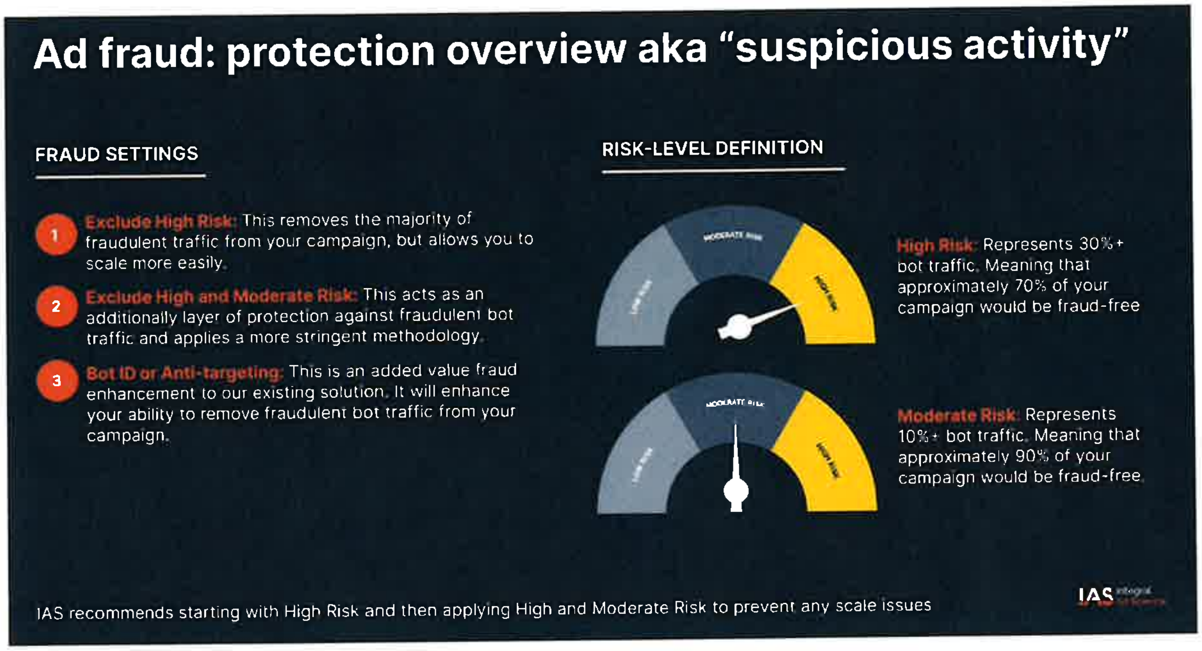
SOLUTIONS THAT DRIVE RESULTS

IAS delivers innovative, industry-leading digital advertising solutions that are designed to drive superior results. Take a look at our full measurement and optimization product suite to learn how IAS helps your brand stay ahead of the competition.

READ MORE

Source: IAS

According to IAS' public documentation, IAS offers a pre-bid segment to prevent ad fraud or "suspicious activity". These segments can help "remove fraudulent bot traffic from your campaign."



Ad fraud: protection overview aka "suspicious activity"

FRAUD SETTINGS

1. **Exclude High Risk:** This removes the majority of fraudulent traffic from your campaign, but allows you to scale more easily.
2. **Exclude High and Moderate Risk:** This acts as an additionally layer of protection against fraudulent bot traffic and applies a more stringent methodology.
3. **Bot ID or Anti-targeting:** This is an added value fraud enhancement to our existing solution. It will enhance your ability to remove fraudulent bot traffic from your campaign.

RISK-LEVEL DEFINITION

High Risk: Represents 30%+ bot traffic. Meaning that approximately 70% of your campaign would be fraud-free

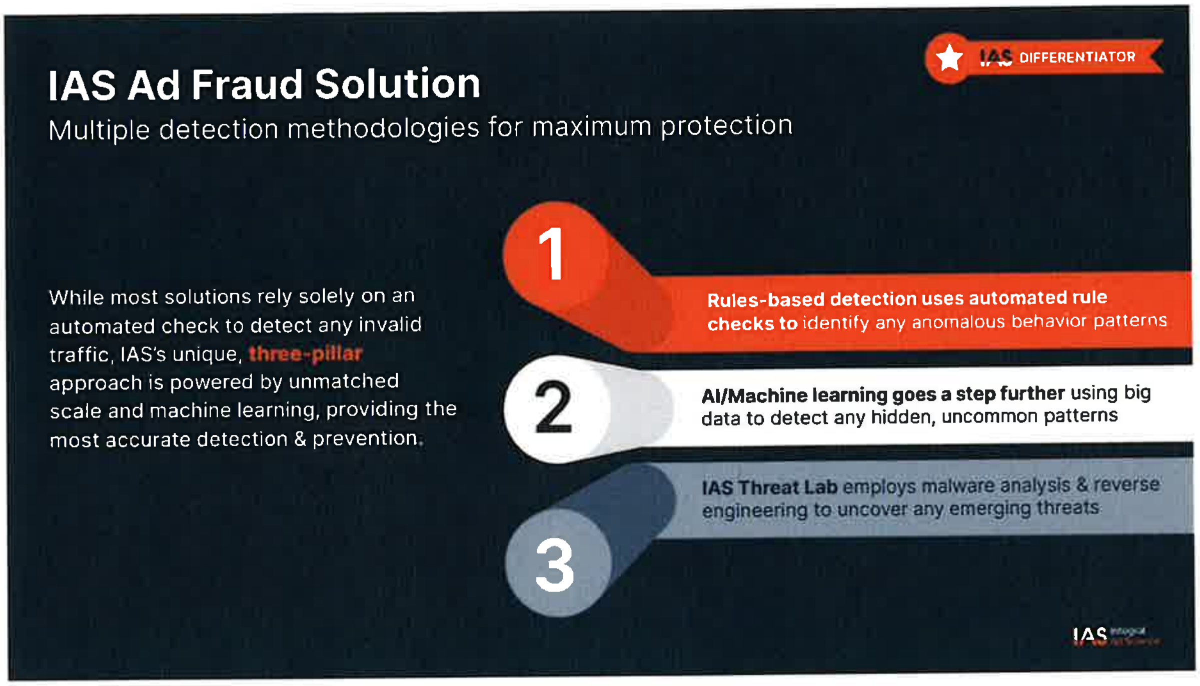
Moderate Risk: Represents 10%+ bot traffic. Meaning that approximately 90% of your campaign would be fraud-free

IAS recommends starting with High Risk and then applying High and Moderate Risk to prevent any scale issues

IAS integral ad science

Screenshot of IAS technical documentation, describing IAS "Suspicious Activity" Pre-Bid Segments; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

According to IAS' public documentation, IAS' Ad Fraud Solution utilized multiple detection methodologies for maximum protection. This three-pillar approach is marketed as being "powered by unmatched scale and machine learning, providing the most accurate detection & prevention." The IAS Ad Fraud Solution claims to use "rules-based detection [...] to identify any anomalous behavior patterns", "AI/Machine Learning [...] using big data to detect any hidden, uncommon patterns", and "malware analysis & reverse engineering to uncover any emerging threats."



IAS DIFFERENTIATOR

IAS Ad Fraud Solution

Multiple detection methodologies for maximum protection

While most solutions rely solely on an automated check to detect any invalid traffic, IAS's unique, **three-pillar** approach is powered by unmatched scale and machine learning, providing the most accurate detection & prevention.

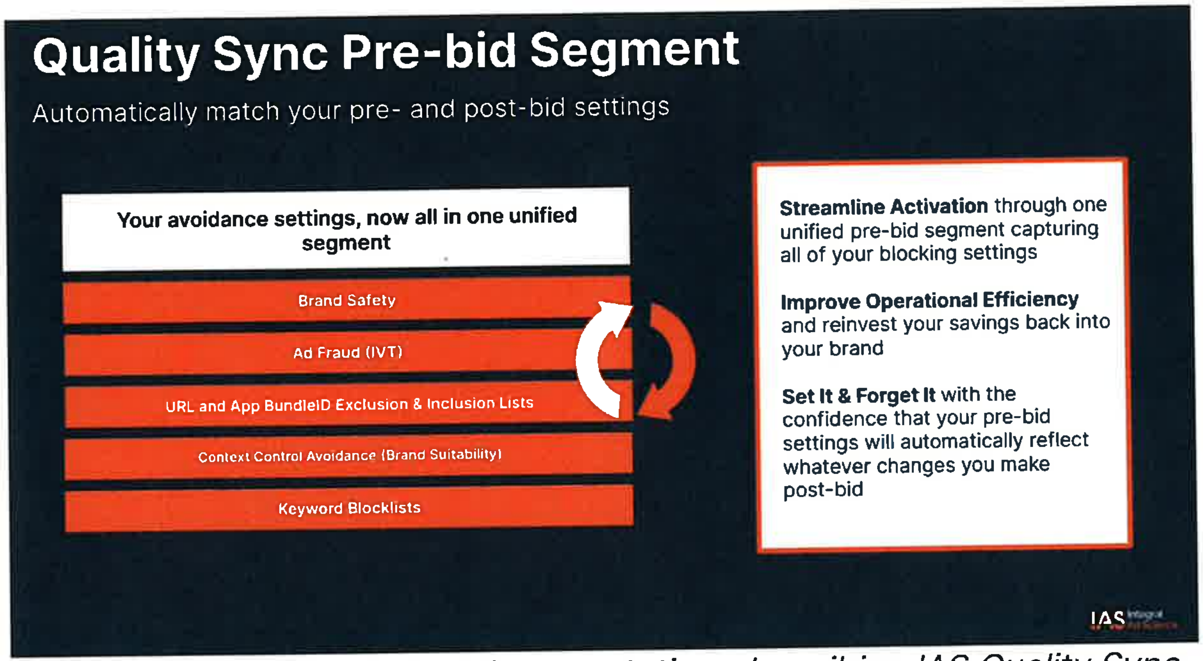
1 **Rules-based detection uses automated rule checks to** identify any anomalous behavior patterns

2 **AI/Machine learning goes a step further** using big data to detect any hidden, uncommon patterns

3 **IAS Threat Lab** employs malware analysis & reverse engineering to uncover any emerging threats

Screenshot of IAS technical documentation, describing IAS Ad Fraud Solution; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

According to IAS' public documentation, IAS offers a "Quality Sync" Pre-bid segment which "automatically matches your pre- and post-bid settings" including "Ad Fraud (IVT)" settings.



Quality Sync Pre-bid Segment

Automatically match your pre- and post-bid settings

Your avoidance settings, now all in one unified segment

- Brand Safety
- Ad Fraud (IVT)
- URL and App BundleID Exclusion & Inclusion Lists
- Context Control Avoidance (Brand Suitability)
- Keyword Blocklists

Streamline Activation through one unified pre-bid segment capturing all of your blocking settings

Improve Operational Efficiency and reinvest your savings back into your brand

Set It & Forget It with the confidence that your pre-bid settings will automatically reflect whatever changes you make post-bid

Screenshot of IAS technical documentation, describing IAS Quality Sync Pre-Bid Segments; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

Background - DoubleVerify ad fraud solutions

DoubleVerify (DV) is an ad verification company that has received multiple Media Rating Council accreditations, and is TAG "Certified Against Fraud". DoubleVerify's website states *"DV analyzes over 2 billion impressions daily, identifying comprehensive fraud and SIVT — from hijacked devices to bot fraud and injected ads. We're accredited by the Media Rating Council (MRC) for monitoring and blocking across devices — including mobile app, and our AI-backed deterministic methodology results in greater accuracy, fewer false positives and, ultimately, superior protection for brands."*

DoubleVerify provides ad verification solutions to both advertisers and to media publishers.

DoubleVerify offers "pre-bid targeting" solutions, which block before an "impression is purchased", including "pre-bid avoidance segments".

DoubleVerify's public website states: *"DV offers the most comprehensive and accurate pre-bid avoidance targeting available in the market. Pre-bid avoidance targeting helps brands drive efficiency from their programmatic media spend by preventing their bidding on auctions misaligned with their ad delivery standards. The solution also helps publishers by preventing the sale of impressions that ultimately result in a block and potential forfeit opportunity [...] Our millions of fraud signatures are updated nearly 100 times per day (every 15 minutes) in our DSP integrations to ensure near-immediate programmatic protection from invalid traffic."*

DoubleVerify further states: *"DV analyzes over 2 billion display and video impressions daily and provides the fastest, most complete fraud identification and protection available — across web, mobile app and CTV environments. Our AI-backed deterministic methodology results in greater accuracy, fewer false positives and, ultimately, superior protection. We pre-qualify your supply to ensure you offer only quality inventory to your advertiser partners — maximizing buyer value and campaign effectiveness. DV works with platform partners in a variety of ways. We can integrate our data directly into your platform to evaluate inventory quality at its source, provide the data needed to package high-quality inventory into easily accessible segments for advertisers, or integrate our metrics into your platform to make optimization easier for buyers. In all instances, you benefit from DV's trusted data, helping to enhance the value and marketability of your inventory."*

Background - Prior research on bot detection and filtration vendors' technology by Shailin Dhar - "Mystery Shopping Inside the Ad Fraud Verification Bubble"

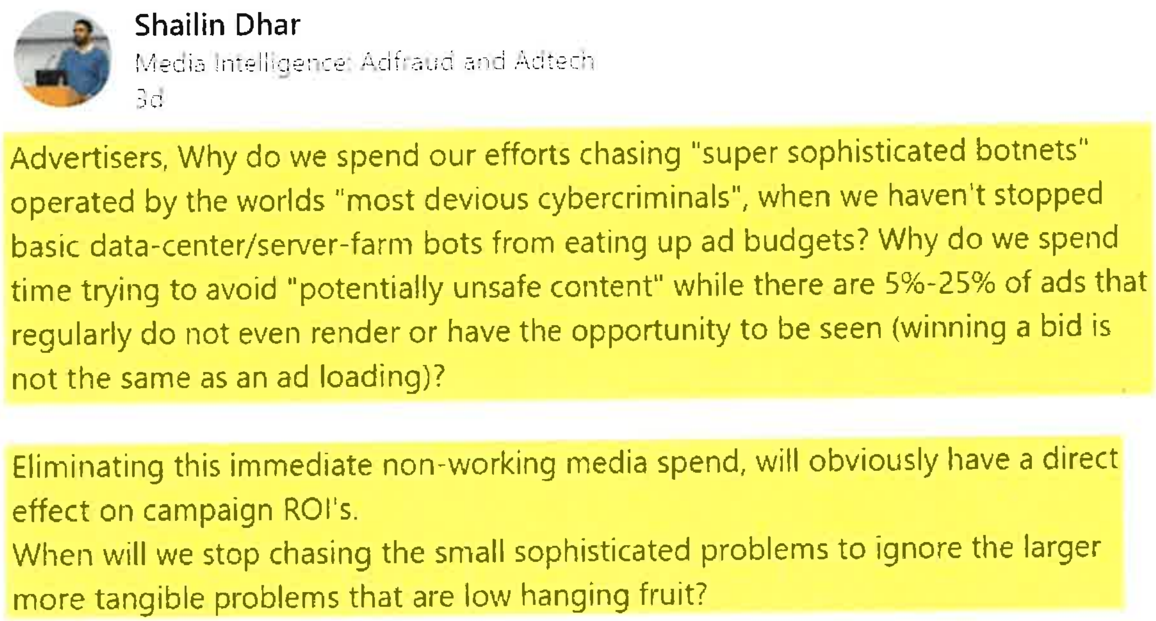
The Financial Times previously cited Shailin Dhar in 2017, an ad tech industry expert, who conducted research on detecting bots and ad fraud.

"Mr. Dhar remains skeptical about how far the industry will get in its fraud-fighting efforts, given that many constituents have a financial incentive to maintain the status quo. "Ad tech companies have made billions of dollars a

year from fraudulent traffic," he says. "Fraud is built into the foundation of advertising supply.""

Shailin Dhar previously commented in a Linkedin post: "

"Advertisers, Why do we spend our efforts chasing "super sophisticated botnets" operated by the worlds "most devious cybercriminals", when we haven't stopped basic data-center/server-farms from eating up ad budgets?"



Shailin Dhar
Media Intelligence: Adfraud and Adtech
3d

Advertisers, Why do we spend our efforts chasing "super sophisticated botnets" operated by the worlds "most devious cybercriminals", when we haven't stopped basic data-center/server-farm bots from eating up ad budgets? Why do we spend time trying to avoid "potentially unsafe content" while there are 5%-25% of ads that regularly do not even render or have the opportunity to be seen (winning a bid is not the same as an ad loading)?

Eliminating this immediate non-working media spend, will obviously have a direct effect on campaign ROI's.
When will we stop chasing the small sophisticated problems to ignore the larger more tangible problems that are low hanging fruit?

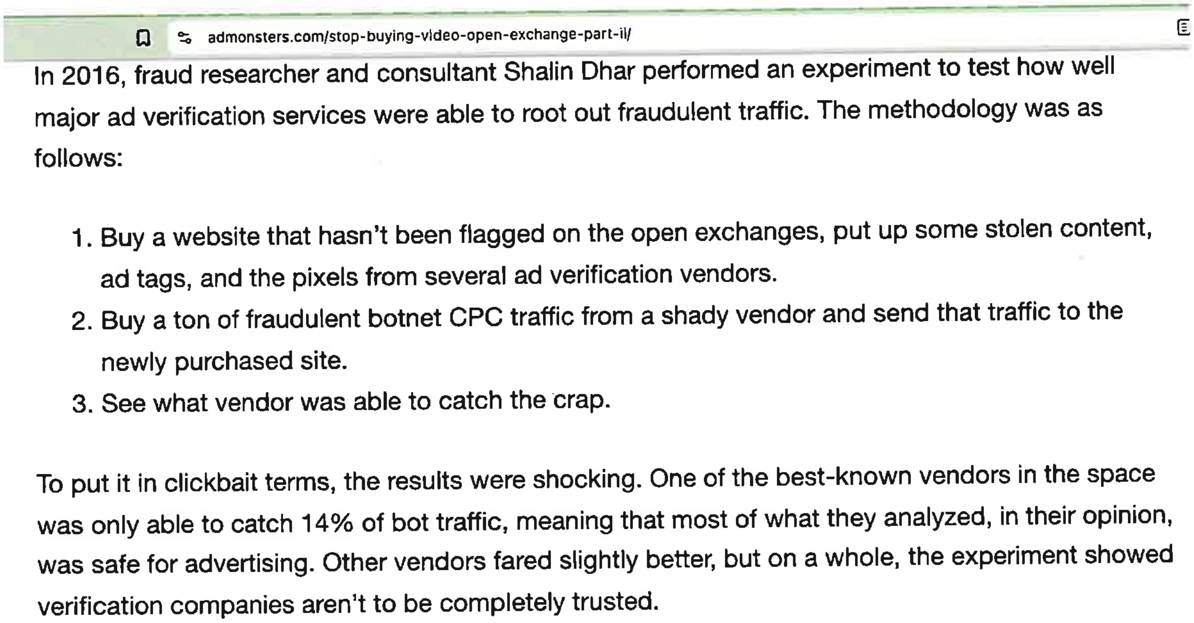
Source: https://www.linkedin.com/pulse/marketers-stop-distracting-yourself-focus-ad-fraud/

According to an AdMonsters article,

"In 2016, fraud researcher and consultant Shailin Dhar performed an experiment to test how well major ad verification services were able to root out fraudulent traffic. The methodology was as follows:

1. *Buy a website that hasn't been flagged on the open exchanges, put up some stolen content, ad tags, and the pixels from several ad verification vendors.*
2. *Buy a ton of fraudulent botnet CPC traffic from a shady vendor and send that traffic to the newly purchased site.*
3. *See what vendor was able to catch the crap.*

To put it in clickbait terms, the results were shocking. One of the best-known vendors in the space was only able to catch 14% of bot traffic, meaning that most of what they analyzed, in their opinion, was safe for advertising. Other vendors fared slightly better, but on a whole, the experiment showed verification companies aren't to be completely trusted."



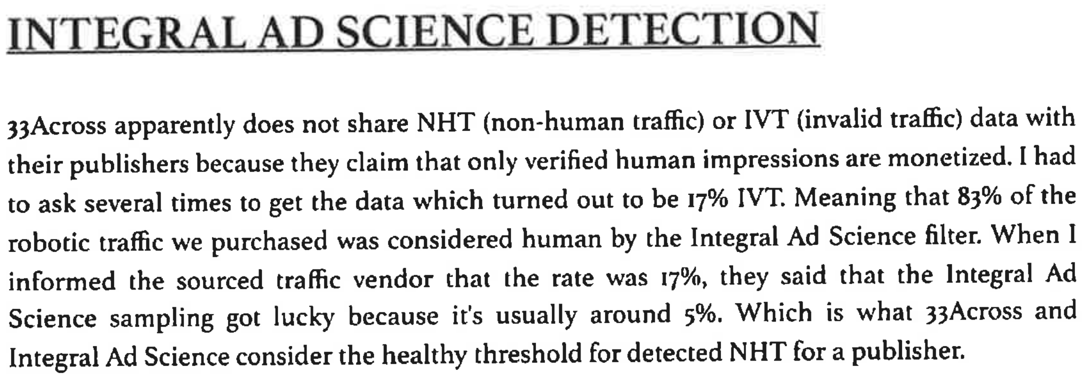
In 2016, fraud researcher and consultant Shalin Dhar performed an experiment to test how well major ad verification services were able to root out fraudulent traffic. The methodology was as follows:

1. Buy a website that hasn't been flagged on the open exchanges, put up some stolen content, ad tags, and the pixels from several ad verification vendors.
2. Buy a ton of fraudulent botnet CPC traffic from a shady vendor and send that traffic to the newly purchased site.
3. See what vendor was able to catch the crap.

To put it in clickbait terms, the results were shocking. One of the best-known vendors in the space was only able to catch 14% of bot traffic, meaning that most of what they analyzed, in their opinion, was safe for advertising. Other vendors fared slightly better, but on a whole, the experiment showed verification companies aren't to be completely trusted.

Screenshot of an AdMonsters.com article from 2017.

According to Shailin Dhar's research from 2017, Integral Ad Science was able to correctly identify only 17% of the bot traffic Mr. Dhar paid to run against an artificial website he created. Mr. Dhar says: "83% of the robotic traffic we purchased was considered human by the Integral Ad Science filter. When I informed the source traffic vendor that the rate was 17% they said that the Integral Ad Science sampling got lucky because it's usually around 5%".



INTEGRAL AD SCIENCE DETECTION

33Across apparently does not share NHT (non-human traffic) or IVT (invalid traffic) data with their publishers because they claim that only verified human impressions are monetized. I had to ask several times to get the data which turned out to be 17% IVT. Meaning that 83% of the robotic traffic we purchased was considered human by the Integral Ad Science filter. When I informed the sourced traffic vendor that the rate was 17%, they said that the Integral Ad Science sampling got lucky because it's usually around 5%. Which is what 33Across and Integral Ad Science consider the healthy threshold for detected NHT for a publisher.

Source: "Mystery Shopping Inside the Ad Fraud Verification Bubble"

Background: US Senators Letters ask Federal Trade Commission to investigate "willful blindness to fraudulent activity in the online ad market"

In 2016, two US Senators - Mark Warner and Chuck Schumer - wrote a letter to the Federal Trade Commission (FTC), asking the agency to take a "*closer look at the negative economic impact of digital advertising fraud on consumers and advertisers*".

According to AdExchanger, the "*senators contend that ad fraud unchecked will trigger a rise in wasted marketing costs that will eventually get passed down to the consumer in the form of higher prices for goods and services.*"

The Senators wrote: "*The cost of pervasive fraud in the digital advertising space will ultimately be paid by the American consumer in the form of higher prices for goods and services [...] It remains to be seen whether voluntary, market-based oversight is sufficient to protect consumers and advertisers.*"

The Senators also asked: "*To the extent that criminal organizations are involved in perpetuating digital advertising fraud, how is the FTC coordinating with both law enforcement (e.g., the Department of Homeland Security or the Federal Bureau of Investigation) and the private sector formulate an appropriate response?*"

The Senators wrote another letter in 2018, saying "*I am writing to express my continued concern with the prevalence of digital advertising fraud, and in particular the inaction of major industry stakeholders in curbing these abuses. In 2016, Senator Schumer and I wrote Chairwoman Ramirez to express frustration with the growing phenomenon of digital ad fraud. Digital ad fraud has only grown since that time*".

The Senators asked the Federal Trade Commission to investigate "*the extent to which major ecosystem stakeholders engage in willful blindness to fraudulent activity in the online ad market.*"

Adalytics public interest research objectives

The following outlines Adalytics' research objectives which are believed to be in the public interest.

1. Did any advertisers have their ads served to bots operating out of data center server farms?
    a. Did any US government or US military advertisers have their ads served to bots by ad tech vendors?
    b. Did any non-profit, NGO, or charity advertisers have their ads served to bots by ad tech vendors?
2. Were any ads served to bots by vendors who made public claims about filtering out bot traffic before an ad impression was served? If so, which vendors who made such public proclamations were observed serving ads to bots?

Research Methodology

This empirical, observational research study did not actively manipulate independent control variables or seek to generate new data. Rather, the study was premised on observing and analyzing data that was already generated by other entities.

Detecting bot traffic is an ever-changing discipline. Bot detection vendors continuously upgrade their detection algorithms, whilst entities who operate bots for benign and malicious purposes seek to circumvent those detections by applying increasingly sophisticated or novel evasions.

This study circumvents the difficulties of accurately detecting bot traffic by instead relying entirely on data wherein the ground truth is universally known. Specifically, this observational research study chose to source 100% of observations and data from three bot operators who are not actively seeking to commit ad fraud.

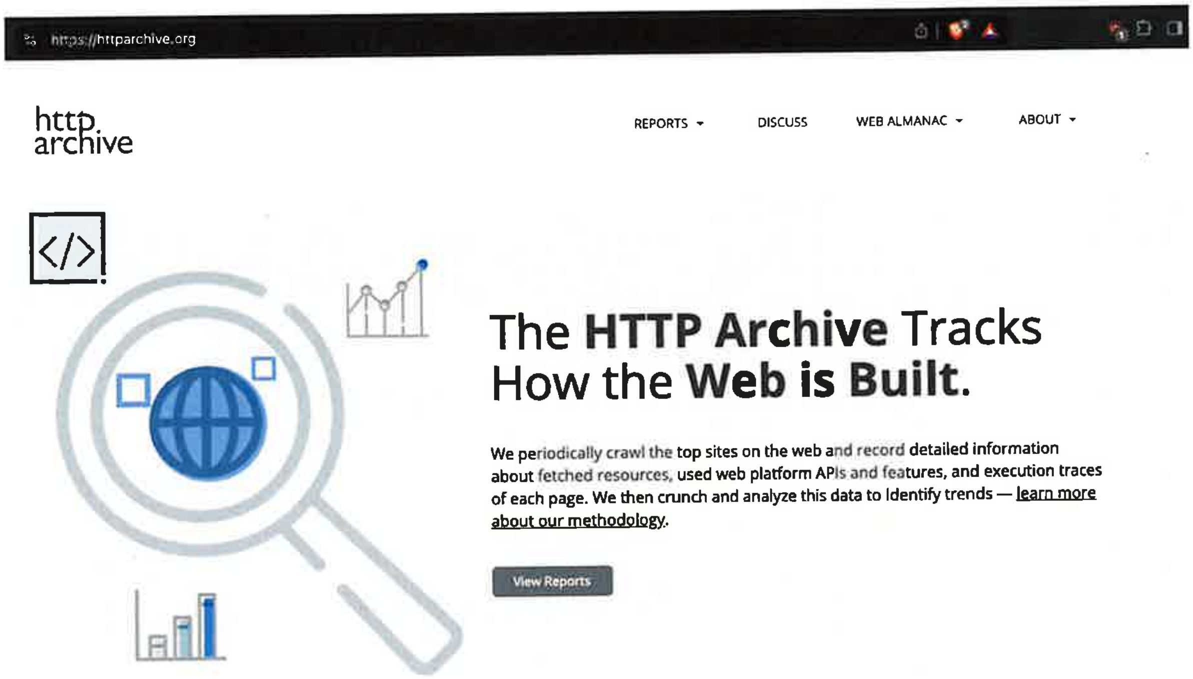
As such, there can be no ambiguity or debate about whether the ads served in these contexts were served to humans or bots; there is absolute certainty that every single one of these ad impressions is confirmed to have been served to a bot, given the provenance of the data.

To the best of our knowledge, this study constitutes the largest analysis of declared bot traffic in the context of digital advertising.

Research Methodology - Bot web traffic source #1 - HTTP Archive

The first source of bot traffic data was HTTP Archive. The HTTP Archive is part of the Internet Archive, a 501(c)(3) non-profit.

The HTTP Archive "Tracks How the Web is Built." HTTP Archive states that they "periodically crawl the top sites on the web and record detailed information about fetched resources, used web platform APIs and features, and execution traces of each page. We then crunch and analyze this data to identify trends — learn more about our methodology."

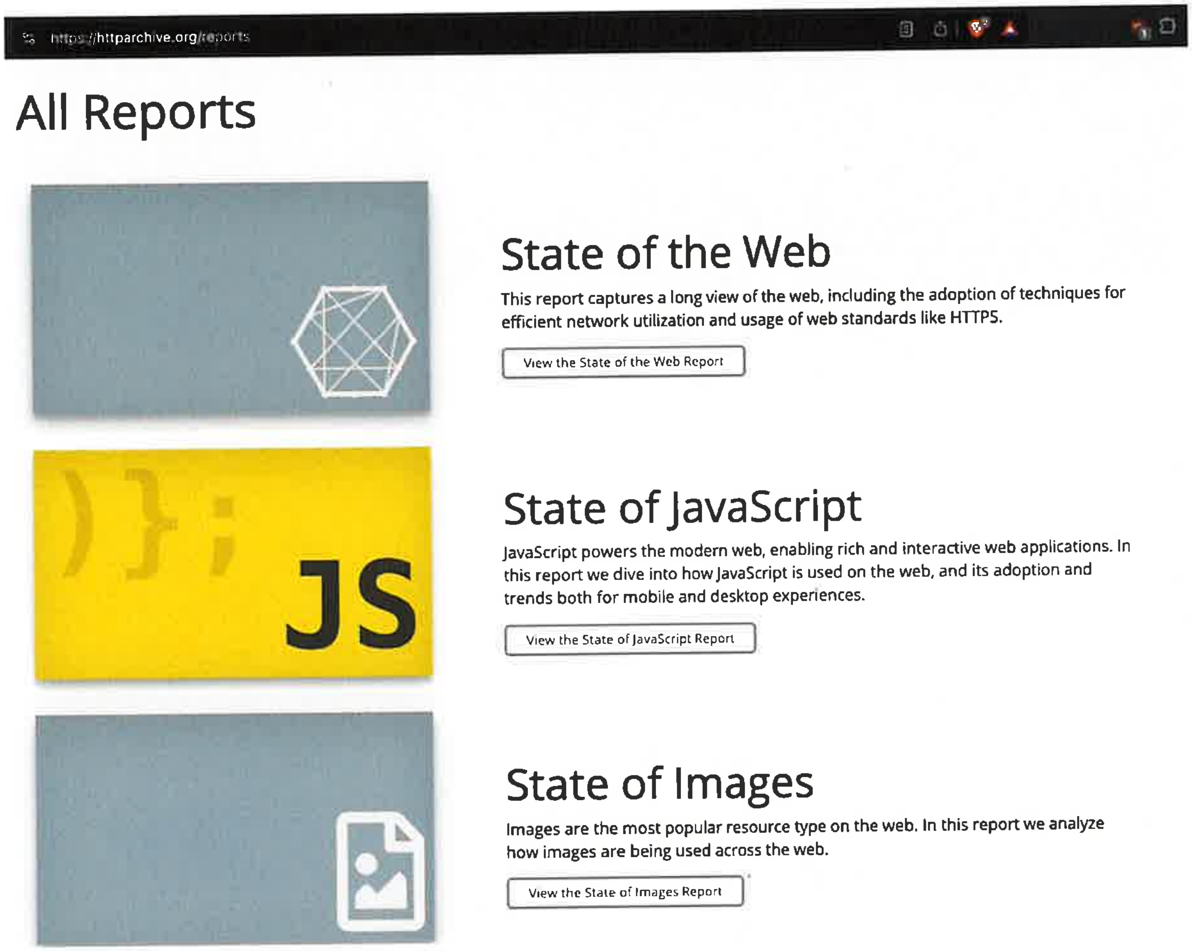


The HTTP Archive Tracks How the Web is Built.

We periodically crawl the top sites on the web and record detailed information about fetched resources, used web platform APIs and features, and execution traces of each page. We then crunch and analyze this data to identify trends — learn more about our methodology.

Screenshot of the HTTP Archive home page - https://httparchive.org/

The HTTP Archive publishes academic research reports about the state of web technology trends on the open internet.


https://httparchive.org/reports
JS
View the State of the Web Report
View the State of JavaScript Report
View the State of Images Report

All Reports

State of the Web

This report captures a long view of the web, including the adoption of techniques for efficient network utilization and usage of web standards like HTTPS.

State of JavaScript

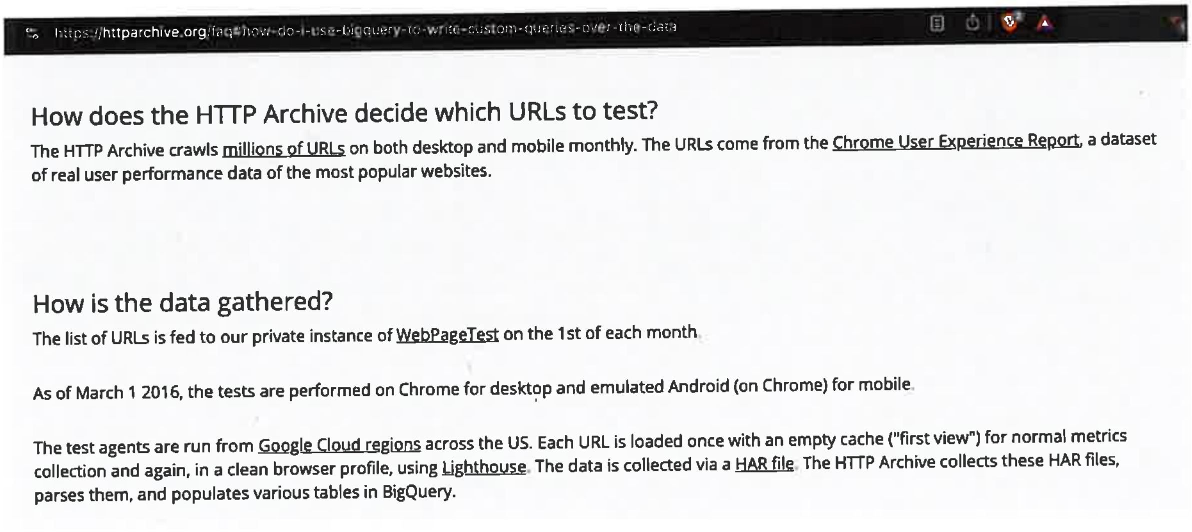
JavaScript powers the modern web, enabling rich and interactive web applications. In this report we dive into how JavaScript is used on the web, and its adoption and trends both for mobile and desktop experiences.

State of Images

Images are the most popular resource type on the web. In this report we analyze how images are being used across the web.

Screenshot of the HTTP Archive "All Reports" page - https://httparchive.org/reports

The HTTP Archive crawls millions of URLs on both desktop and mobile monthly. "The URLs come from the Chrome User Experience Report, a dataset of real user performance data of the most popular websites. The list of URLs is fed to our private instance of WebPageTest on the 1st of each month. As of March 1 2016, the tests are performed on Chrome for desktop and emulated Android (on Chrome) for mobile. The test agents are run from Google Cloud regions across the US. Each URL is loaded once with an empty cache ("first view") for normal metrics collection and again, in a clean browser profile, using Lighthouse. The data is collected via a HAR file. The HTTP Archive collects these HAR files, parses them, and populates various tables in BigQuery.


https://httparchive.org/faq#how-do-i-use-bigquery-to-write-custom-queries-over-the-data

How does the HTTP Archive decide which URLs to test?

The HTTP Archive crawls millions of URLs on both desktop and mobile monthly. The URLs come from the Chrome User Experience Report, a dataset of real user performance data of the most popular websites.

How is the data gathered?

The list of URLs is fed to our private instance of WebPageTest on the 1st of each month.

As of March 1 2016, the tests are performed on Chrome for desktop and emulated Android (on Chrome) for mobile.

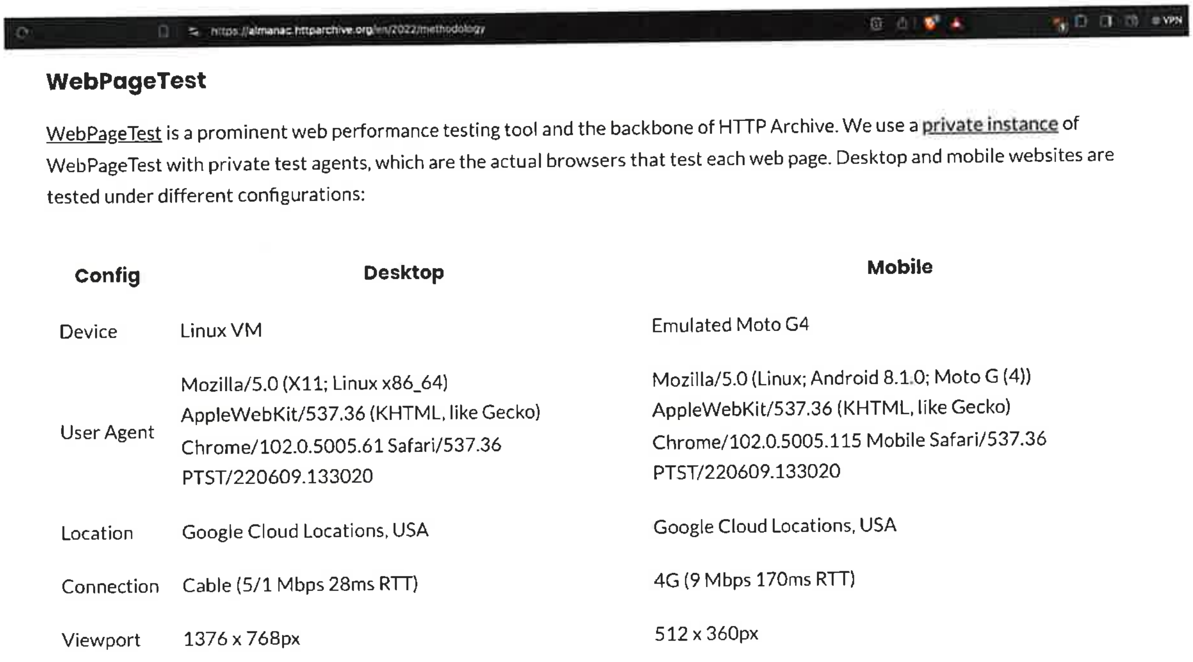
The test agents are run from Google Cloud regions across the US. Each URL is loaded once with an empty cache ("first view") for normal metrics collection and again, in a clean browser profile, using Lighthouse. The data is collected via a HAR file. The HTTP Archive collects these HAR files, parses them, and populates various tables in BigQuery.

Screenshot of the HTTP Archive's FAQ page - https://httparchive.org/faq

The HTTP Archive crawls websites using desktop and mobile user agents. Per the HTTP Archive's methodology, it crawls from Google Cloud data centers. The HTTP Archive openly and transparently declares its crawlers via the HTTP User Agent request header. Specifically, HTTP Archive declares that its crawlers declare the following desktop and mobile user-agents:

- Desktop: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 **PTST**/220609.133020
- Mobile: Mozilla/5.0 (Linux; Android 8.1.0; Moto G (4)) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.115 Mobile Safari/537.36 **PTST**/220609.133020

https://adalytics.io/blog/prebid-bot-filtration



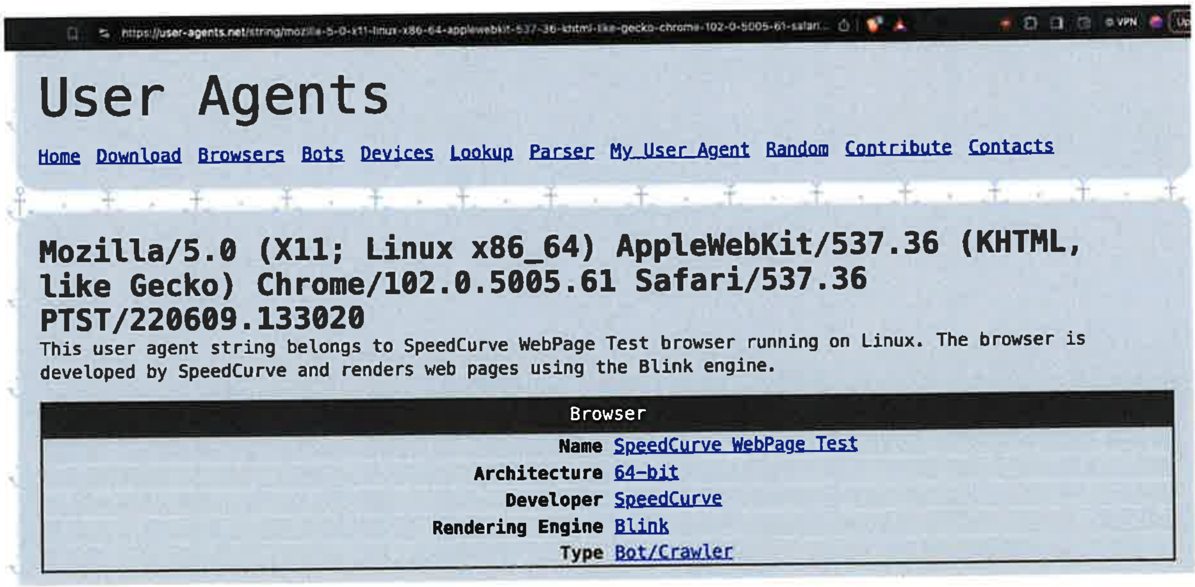
WebPageTest

WebPageTest is a prominent web performance testing tool and the backbone of HTTP Archive. We use a private instance of WebPageTest with private test agents, which are the actual browsers that test each web page. Desktop and mobile websites are tested under different configurations:

Config	Desktop	Mobile
Device	Linux VM	Emulated Moto G4
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020	Mozilla/5.0 (Linux; Android 8.1.0; Moto G (4)) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.115 Mobile Safari/537.36 PTST/220609.133020
Location	Google Cloud Locations, USA	Google Cloud Locations, USA
Connection	Cable (5/1 Mbps 28ms RTT)	4G (9 Mbps 170ms RTT)
Viewport	1376 x 768px	512 x 360px

Screenshot of the HTTP Archive's methodology page - https://almanac.httparchive.org/en/2022/methodology

"PTST" is a well known and established bot user agent. One can check the publicly available user-agent.net database to confirm that "PTST" appears as a "Bot/Crawler".


https://user-agents.net/string/mozilla-5-0-x11-linux-x86-64-applewebkit-537-36-khtml-like-gecko-chrome-102-0-5005-61-safari...
VPN

User Agents

Home Download Browsers Bots Devices Lookup Parser My User Agent Random Contribute Contacts

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020

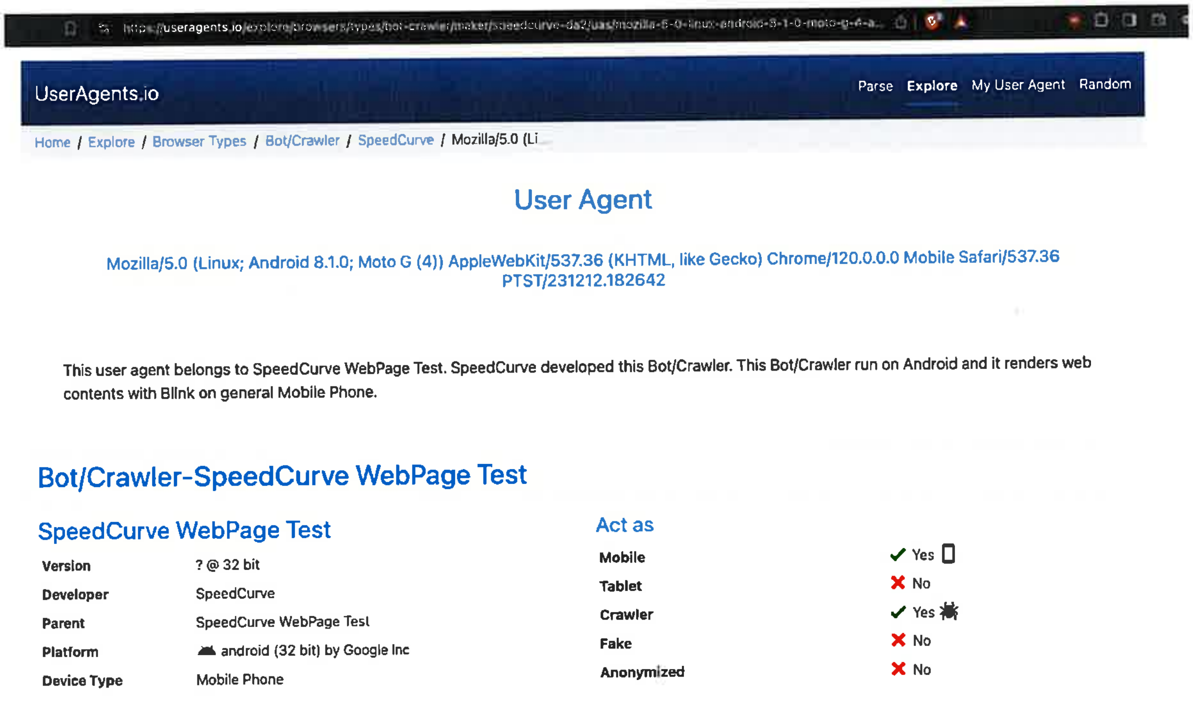
This user agent string belongs to SpeedCurve WebPage Test browser running on Linux. The browser is developed by SpeedCurve and renders web pages using the Blink engine.

Browser	
Name	SpeedCurve WebPage Test
Architecture	64-bit
Developer	SpeedCurve
Rendering Engine	Blink
Type	Bot/Crawler

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Screenshot of the User-Agents.net database, showing that "PTST" is a known "Bot/Crawler" - https://user-agents.net/string/mozilla-5-0-x11-linux-x86-64-applewebkit-537-36-khtml-like-gecko-chrome-102-0-5005-61-safari-537-36-ptst-220609-133020

UserAgents.io - another public user agent database - also confirms that "PTST" is a known Crawler.


https://useragents.io/explore/browsers/types/bot-crawler/maker/speedcurve-da2/uas/mozilla-5-0-linux-android-8-1-0-moto-g-4-a...
UserAgents.io
Parse
Explore
My User Agent
Random
Home / Explore / Browser Types / Bot/Crawler / SpeedCurve / Mozilla/5.0 (Li

User Agent

Mozilla/5.0 (Linux; Android 8.1.0; Moto G (4)) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Mobile Safari/537.36 PTST/231212.182642

This user agent belongs to SpeedCurve WebPage Test. SpeedCurve developed this Bot/Crawler. This Bot/Crawler run on Android and it renders web contents with Blink on general Mobile Phone.

Bot/Crawler-SpeedCurve WebPage Test

SpeedCurve WebPage Test

Version	? @ 32 bit
Developer	SpeedCurve
Parent	SpeedCurve WebPage Test
Platform	android (32 bit) by Google Inc
Device Type	Mobile Phone

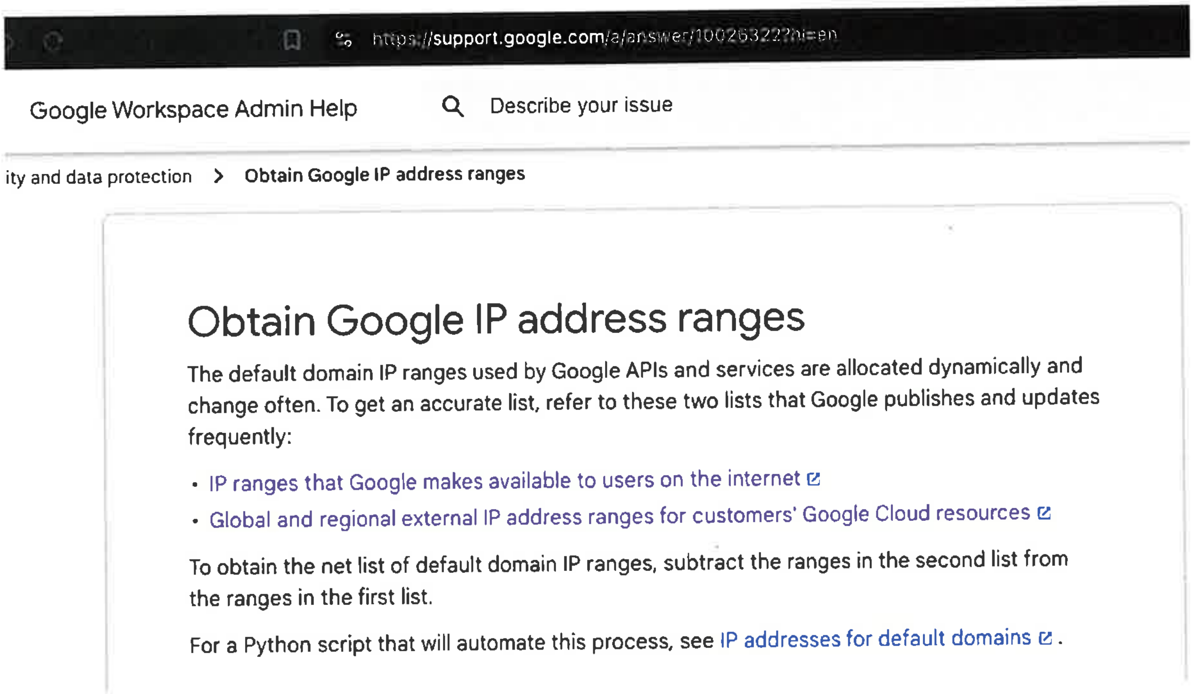
Act as

Mobile	✓ Yes
Tablet	✗ No
Crawler	✓ Yes
Fake	✗ No
Anonymized	✗ No

Screenshot of UserAgents.io - another public user agent database - showing that "PTST" is a known Crawler.

"PTST" has also been on the IAB Tech Lab Spiders and Bots robots list since 2013. "*The IAB Tech Lab publishes a comprehensive list of such Spiders and Robots that helps companies identify automated traffic such as search engine crawlers, monitoring tools, and other non-human traffic that they don't want included in their analytics and billable counts.*" The "*spiders and robots list supports the MRC's General Invalid Traffic Detection and Filtration Standard by providing a common industry resource and list for facilitating IVT detection and filtration.*"

HTTP Archive crawls from Google Cloud data center server farms. The IPs operated by Google Cloud are publicly documented on Google's website - https://support.google.com/a/answer/10026322?hl=en


https://support.google.com/a/answer/10026322?hl=en
Google Workspace Admin Help
Describe your issue
ity and data protection > Obtain Google IP address ranges

Obtain Google IP address ranges

The default domain IP ranges used by Google APIs and services are allocated dynamically and change often. To get an accurate list, refer to these two lists that Google publishes and updates frequently:

- IP ranges that Google makes available to users on the internet
- Global and regional external IP address ranges for customers' Google Cloud resources

To obtain the net list of default domain IP ranges, subtract the ranges in the second list from the ranges in the first list.

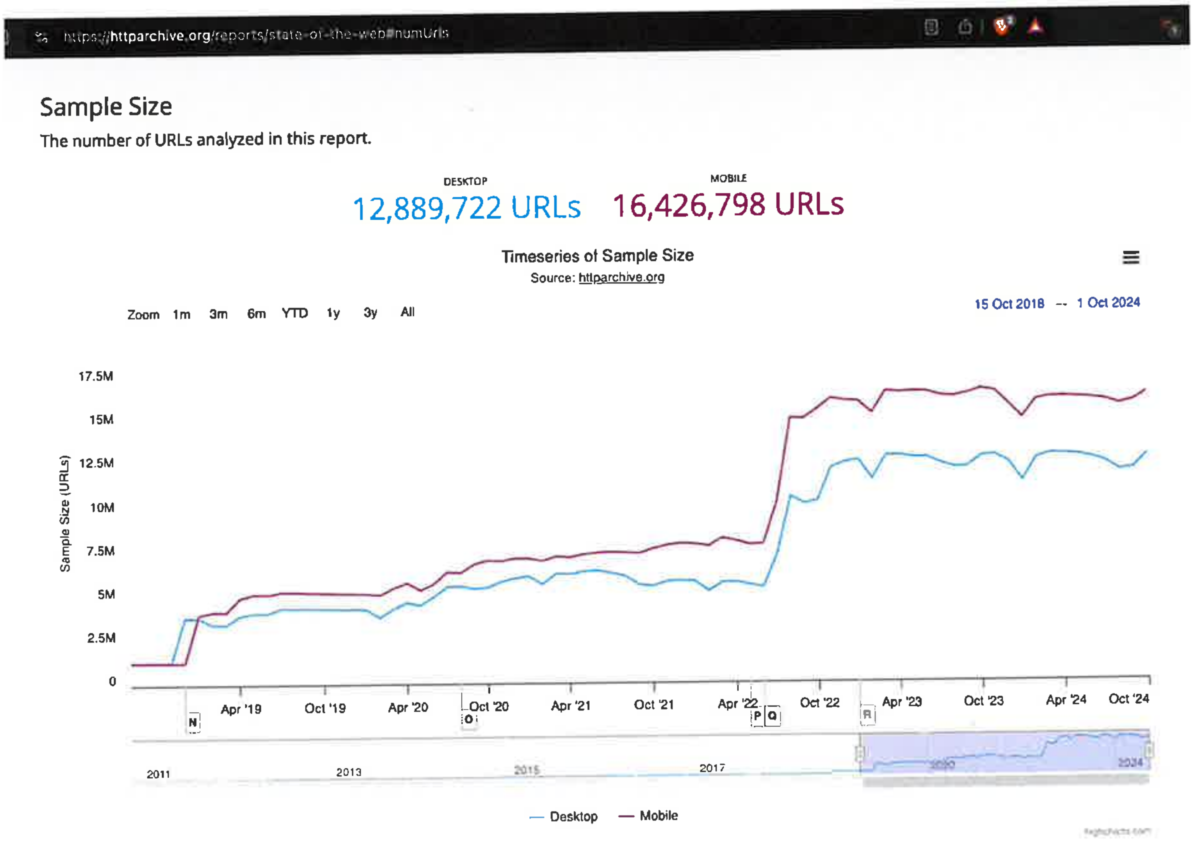
For a Python script that will automate this process, see IP addresses for default domains .

Screenshot of Google's public documentation, showing how one can obtain Google Cloud's IP address ranges

As a reminder, the Media Rating Council (MRC) - an advertising accreditation body says "*requiring filtration of invalid data-center traffic originating from IPs associated to the three largest known hosting entities: Amazon AWS, **Google** and Microsoft. This means filtration of IPs within those of known hosting entities determined to be a consistent source of invalid traffic not including routing artifacts of legitimate users or virtual machine legitimate browsing*" (emphasis added).

The HTTP Archive has crawled tens of millions of distinct page URLs over the course of several years.

https://adalytics.io/blog/prebid-bot-filtration



https://httparchive.org/reports/state-of-the-web#numUrls

Sample Size

The number of URLs analyzed in this report.

DESKTOP 12,889,722 URLs

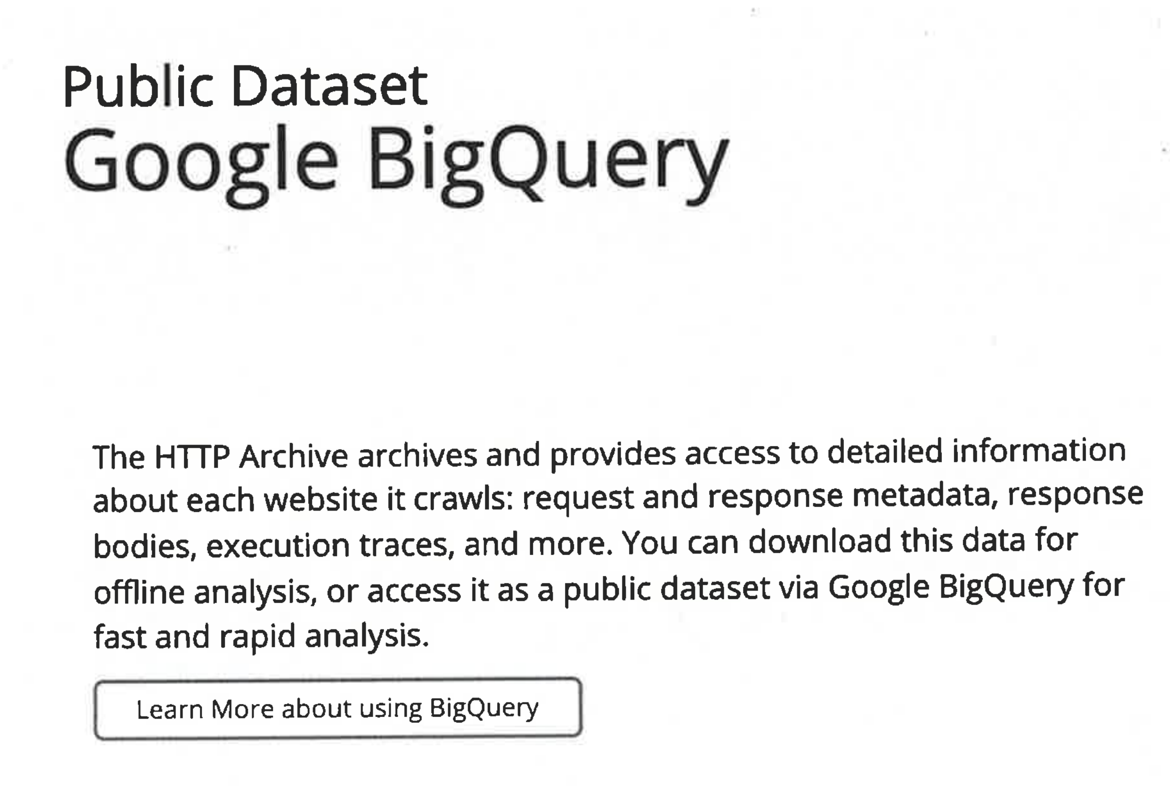
MOBILE 16,426,798 URLs

Timeseries of Sample Size

Source: httparchive.org

Screenshot of the HTTP Archive Reports section, showing how many page URLs are crawled - https://httparchive.org/reports/state-of-the-web#numUrls

The HTTP Archive makes peta-bytes of web traffic data generated through its crawls as a Public Dataset on Google BigQuery.



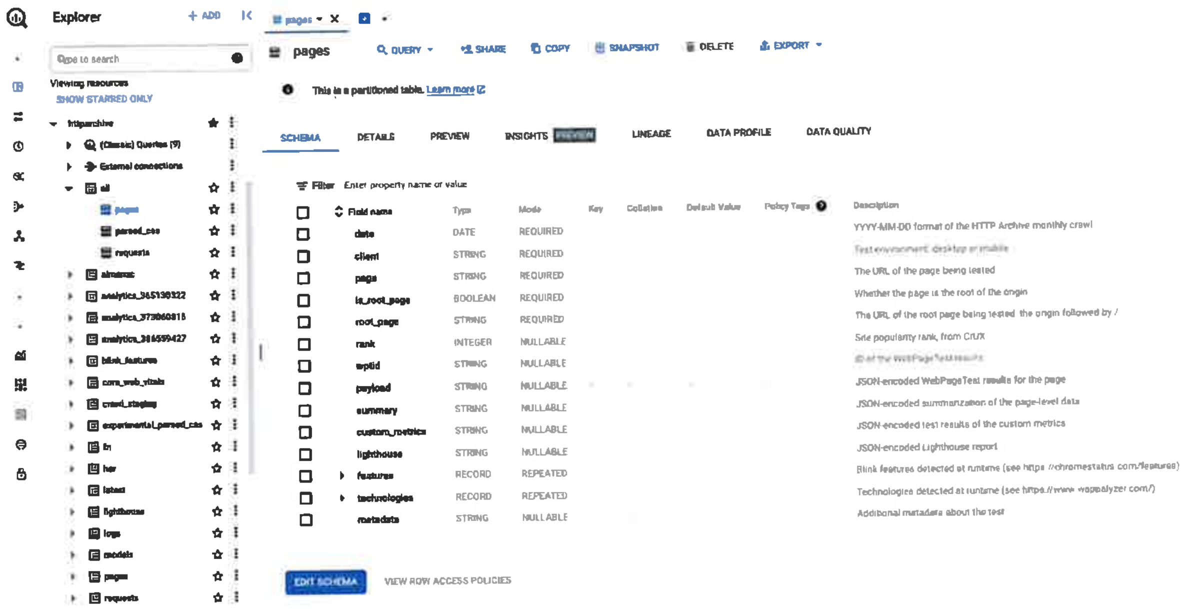
Public Dataset

Google BigQuery

The HTTP Archive archives and provides access to detailed information about each website it crawls: request and response metadata, response bodies, execution traces, and more. You can download this data for offline analysis, or access it as a public dataset via Google BigQuery for fast and rapid analysis.

Screenshot of the HTTP Archive Google BigQuery dataset - https://httparchive.org/faq#how-do-i-use-bigquery-to-write-custom-queries-over-the-data

In the screenshot below, one can see examples of how a user can interface with and query the HTTP Archive dataset.

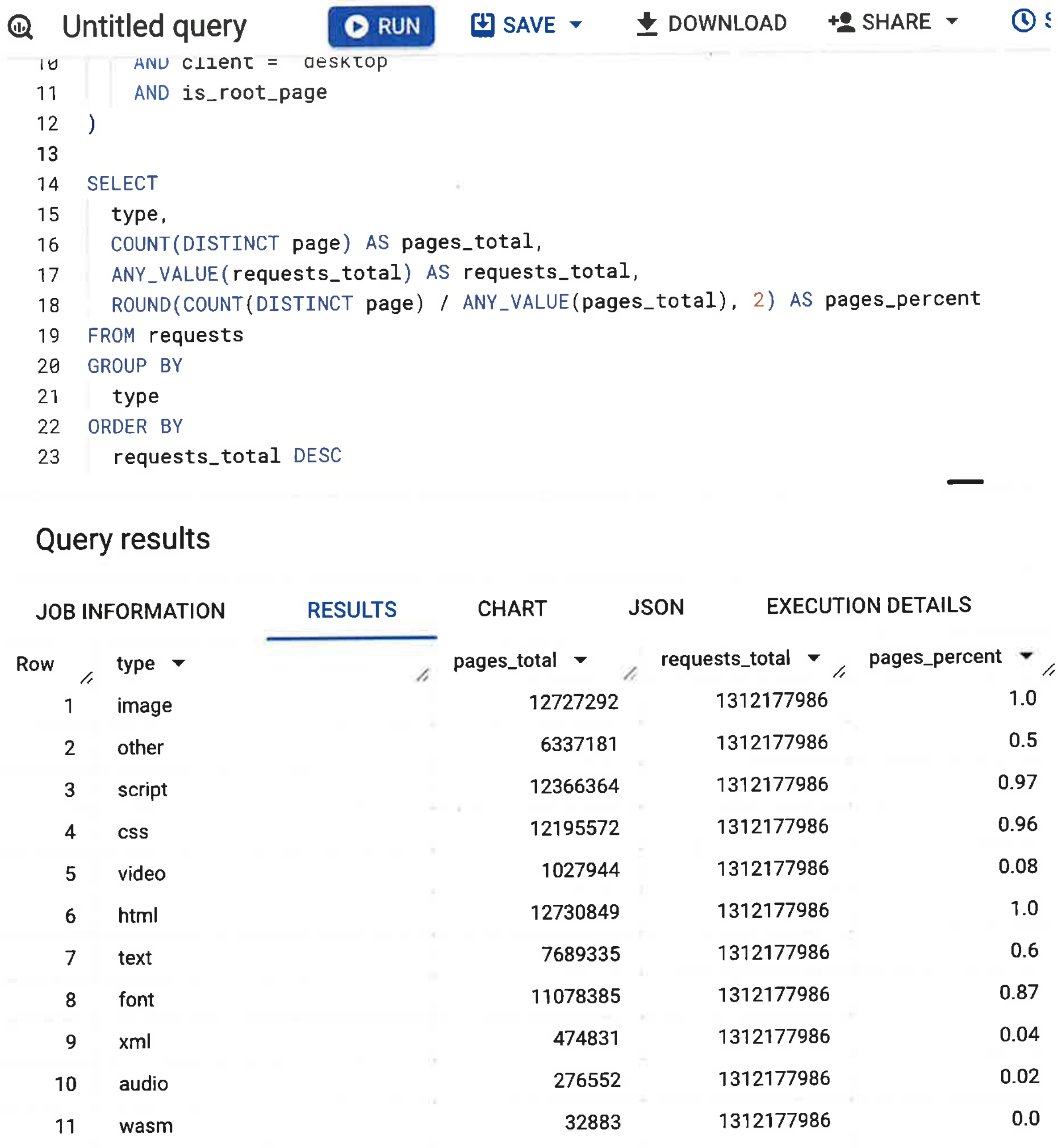


This is a partitioned table. Learn more

Filter Enter property name or value

□	Field name	Type	Mode	Key	Collation	Default Value	Policy Tags	Description
□	date	DATE	REQUIRED					YYYY-MM-DD format of the HTTP Archive monthly crawl
□	client	STRING	REQUIRED					Test environment: desktop or mobile
□	page	STRING	REQUIRED					The URL of the page being tested
□	is_root_page	BOOLEAN	REQUIRED					Whether the page is the root of the origin
□	root_page	STRING	REQUIRED					The URL of the root page being tested, the origin followed by /
□	rank	INTEGER	NULLABLE					Site popularity rank, from CrUX
□	wptid	STRING	NULLABLE					ID of the WebPageTest results
□	payload	STRING	NULLABLE					JSON-encoded WebPageTest results for the page
□	summary	STRING	NULLABLE					JSON-encoded summarization of the page-level data
□	custom_metrics	STRING	NULLABLE					JSON-encoded test results of the custom metrics
□	lighthouse	STRING	NULLABLE					JSON-encoded Lighthouse report
□	features	RECORD	REPEATED					Blink features detected at runtime (see https://chromestatus.com/features)
□	technologies	RECORD	REPEATED					Technologies detected at runtime (see https://www.wappalyzer.com/)
□	metadata	STRING	NULLABLE					Additional metadata about the test

Example screenshot showing how to use Google BigQuery to query the public HTTP Archive dataset - https://har.fyi/guides/getting-started/



```
    AND client =  desktop
    AND is_root_page
)

SELECT
  type,
  COUNT(DISTINCT page) AS pages_total,
  ANY_VALUE(requests_total) AS requests_total,
  ROUND(COUNT(DISTINCT page) / ANY_VALUE(pages_total), 2) AS pages_percent
FROM requests
GROUP BY
  type
ORDER BY
  requests_total DESC
```

Row	type	pages_total	requests_total	pages_percent
1	image	12727292	1312177986	1.0
2	other	6337181	1312177986	0.5
3	script	12366364	1312177986	0.97
4	css	12195572	1312177986	0.96
5	video	1027944	1312177986	0.08
6	html	12730849	1312177986	1.0
7	text	7689335	1312177986	0.6
8	font	11078385	1312177986	0.87
9	xml	474831	1312177986	0.04
10	audio	276552	1312177986	0.02
11	wasm	32883	1312177986	0.0

Example screenshot showing how to use Google BigQuery to query the public HTTP Archive dataset - https://har.fyi/guides/getting-started/

Querying the HTTP Archive dataset allows one to observe whether specific ad tech vendors transacted and/or served ads to declared bots in a known Google Cloud data center.

The Media Rating Council (MRC) states in its "Invalid Traffic Detection and Filtration Standards Addendum" that the "*MRC is requiring filtration of invalid data-center traffic originating from IPs associated to the three largest known hosting entities: Amazon AWS, **Google** and Microsoft*" (emphasis added).

Research Methodology - Bot web traffic source #2 - Anonymous web crawler vendor

The second bot dataset analyzed for the purposes of this research report came from an anonymous web crawler vendor. This vendor shared their web crawling data under condition of anonymity. The vendor crawls the web for various benign reasons - their purpose is not to commit ad fraud or generate ad revenue.

The given vendor crawls approximately seven million websites each month, from several dozen known data center IP addresses, such as Hertzner and Linode data center IPs.

The vendor does not declare via its user-agent HTTP request header that it is a bot; instead, the vendor declares "valid, human" browser user agents when visiting various websites. Thus, the bot's user HTTP User-Agent request header would likely not be located on the IAB's list of known bots and spiders. The bot utilizes different IP addresses when initiating its crawl. The bot will occasionally scan the web from data center IPs as well as from residential proxy IPs. Thus, this bot's browsing activity may possibly in some cases meet the MRC definition of "Sophisticated Invalid Traffic" (SIVT).

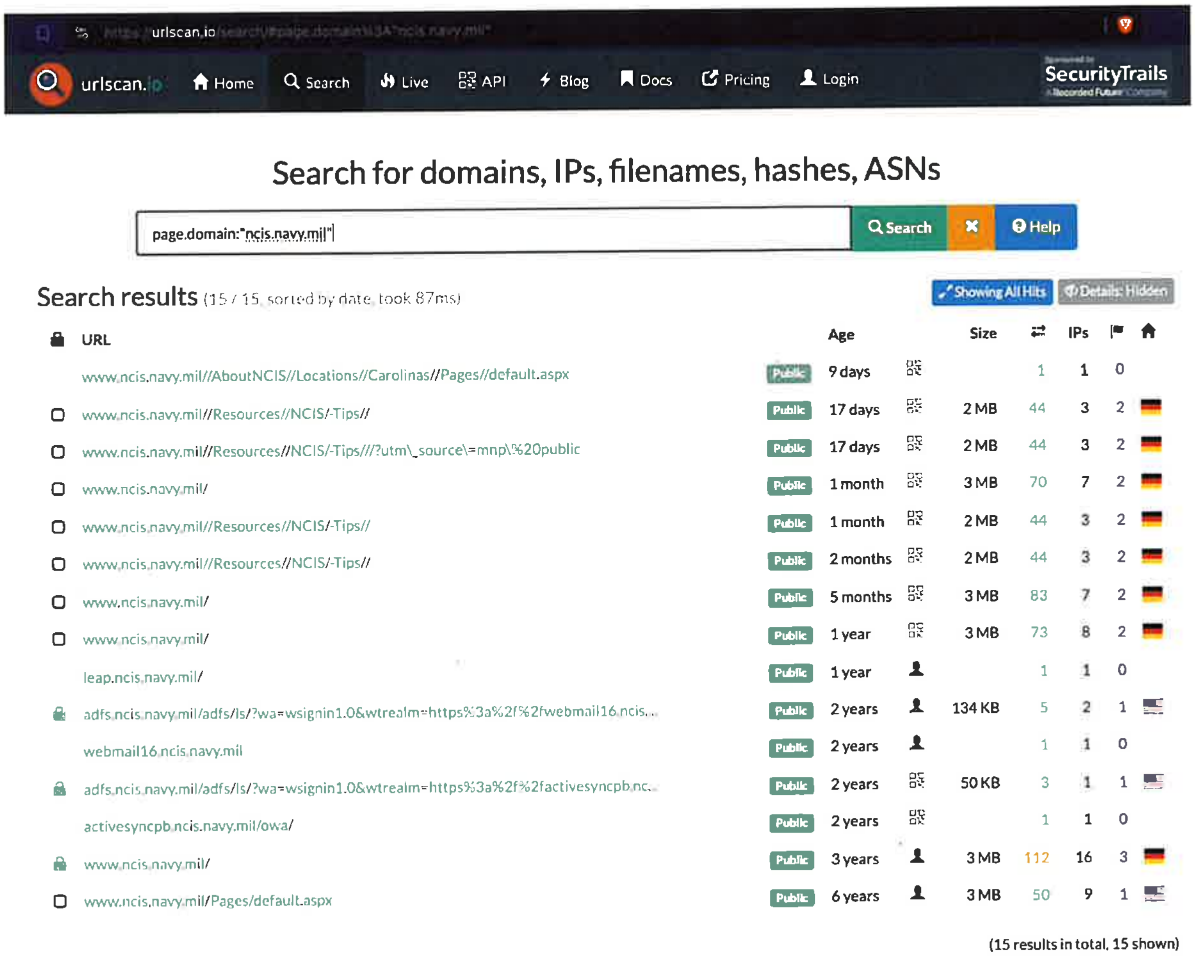
Research Methodology - Bot web traffic source #3 - URLScan.io

The third bot dataset used for this empirical research report was URLScan.io. URLScan.io is a "website scanner for suspicious and malicious URLs." Its mission is to "allow anyone to easily and confidently analyze unknown and potentially malicious websites."

"When a URL is submitted to urlscan.io, an automated process will browse to the URL like a regular user and record the activity that this page navigation creates. This includes the domains and IPs contacted, the resources (JavaScript, CSS, etc) requested from those domains, as well as additional information about the page itself. urlscan.io will take a screenshot of the page, record the DOM content, JavaScript global variables, cookies created by the page, and a myriad of other observations."

URLScan.io does not always declare via its user-agent HTTP header that it is a bot; instead, the vendor's bot appears to declare "valid, human" browser user agents sometimes when visiting various websites. For example, the URLScan.io bot will declare itself to be a "normal" Chrome browser on a Windows or Linux desktop machine, rather than identifying itself as a bot. Thus, in some cases the URLScan.io's bot's HTTP user-agent request header would likely not be found on the IAB's list of known bots and spiders. Furthermore, the URLScan.io bot appears to utilize different IP addresses when initiating its crawl. URLScan.io appears to occasionally scan the web from data center IPs as well as from datacenter-based Virtual Private Network (VPN) or residential proxy IPs. Thus, ads served to URLScan.io's crawler may possibly in some cases meet the MRC definition of "Sophisticated Invalid Traffic" (SIVT).

URLScan.io has a powerful search API that allows users to look for specific previous or historical URLScan.io bot crawls. For example, in the screenshot below, one can see a search to find all instances where URLScan.io scanned the website of the Naval Criminal Investigative Service (ncis.navy.mil). One can see that URLScan.io scanned the NCIS website fifteen times in the last six years.



Search for domains, IPs, filenames, hashes, ASNs

page.domain:"ncis.navy.mil"

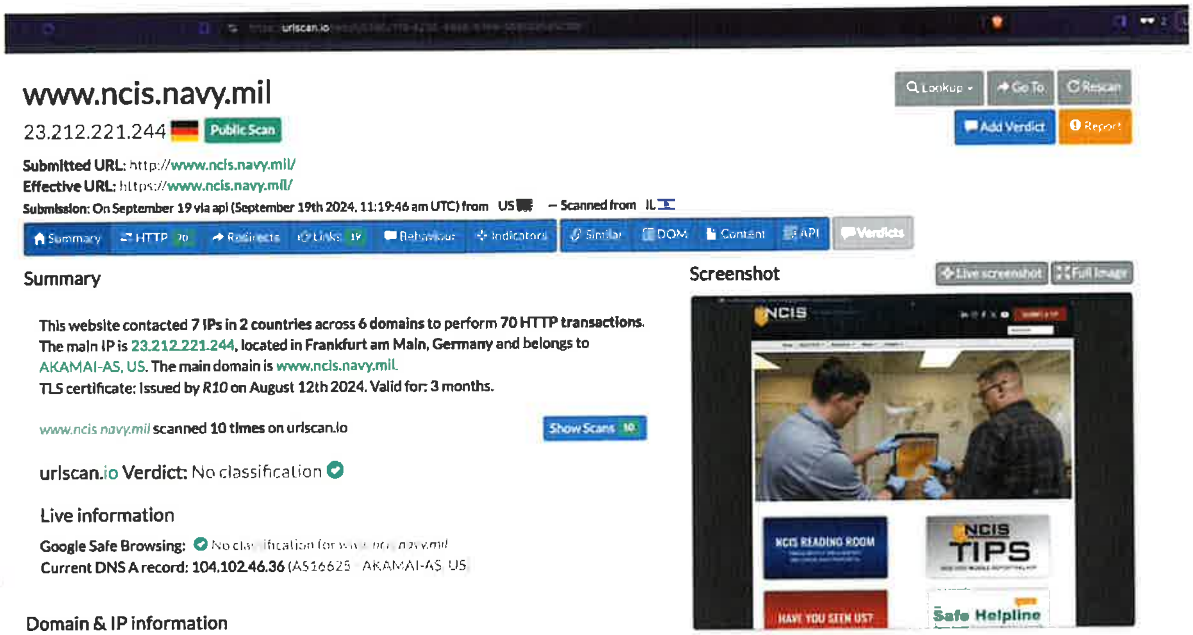
Search results (15 / 15, sorted by date, took 87ms)

🔒	URL		Age		Size	⇄	IPs	⚑	🏠
	www.ncis.navy.mil//AboutNCIS//Locations//Carolinas//Pages//default.aspx	Public	9 days			1	1	0	
□	www.ncis.navy.mil//Resources//NCIS/-Tips//	Public	17 days		2 MB	44	3	2	🇩🇪
□	www.ncis.navy.mil//Resources//NCIS/-Tips///?utm_source\=mnp\%20public	Public	17 days		2 MB	44	3	2	🇩🇪
□	www.ncis.navy.mil/	Public	1 month		3 MB	70	7	2	🇩🇪
□	www.ncis.navy.mil//Resources//NCIS/-Tips//	Public	1 month		2 MB	44	3	2	🇩🇪
□	www.ncis.navy.mil//Resources//NCIS/-Tips//	Public	2 months		2 MB	44	3	2	🇩🇪
□	www.ncis.navy.mil/	Public	5 months		3 MB	83	7	2	🇩🇪
□	www.ncis.navy.mil/	Public	1 year		3 MB	73	8	2	🇩🇪
	leap.ncis.navy.mil/	Public	1 year	👤		1	1	0	
🔒	adfs.ncis.navy.mil/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fwebmail16.ncis...	Public	2 years	👤	134 KB	5	2	1	🇺🇸
	webmail16.ncis.navy.mil	Public	2 years	👤		1	1	0	
🔒	adfs.ncis.navy.mil/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2factivesyncpb.nc...	Public	2 years		50 KB	3	1	1	🇺🇸
	activesyncpb.ncis.navy.mil/owa/	Public	2 years			1	1	0	
🔒	www.ncis.navy.mil/	Public	3 years	👤	3 MB	112	16	3	🇩🇪
□	www.ncis.navy.mil/Pages/default.aspx	Public	6 years	👤	3 MB	50	9	1	🇺🇸

(15 results in total, 15 shown)

Screenshot of URLScan.io's search page, showing fifteen instances where URLScan.io's bot scanned and screenshotted the NCIS website.

One can click on each individual URLScan.io scan to visualize the results of that scan. For example, one can see that URLScan.io's bot crawled ncis.navy.mil on September 19th, 2024, and created a screenshot of the page.



www.ncis.navy.mil

23.212.221.244 Public Scan

Submitted URL: http://www.ncis.navy.mil/
Effective URL: https://www.ncis.navy.mil/
Submission: On September 19 via api (September 19th 2024, 11:19:46 am UTC) from US — Scanned from IL

Summary

This website contacted 7 IPs in 2 countries across 6 domains to perform 70 HTTP transactions. The main IP is 23.212.221.244, located in Frankfurt am Main, Germany and belongs to AKAMAI-AS, US. The main domain is www.ncis.navy.mil.
TLS certificate: Issued by R10 on August 12th 2024. Valid for: 3 months.

www.ncis.navy.mil scanned 10 times on urlscan.io Show Scans 10

urlscan.io Verdict: No classification

Live information

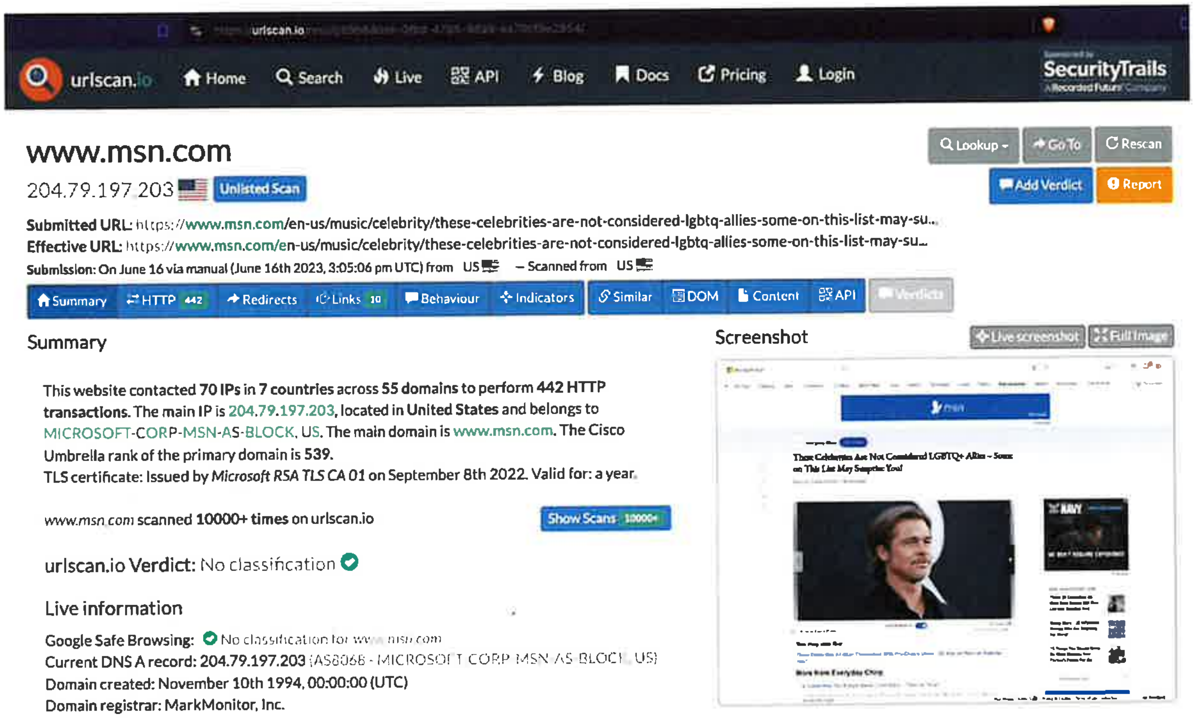
Google Safe Browsing: No classification for www.ncis.navy.mil
Current DNS A record: 104.102.46.36 (AS16625 - AKAMAI-AS, US)

Domain & IP information

Screenshot

Screenshot of a URLScan.io bot crawling and screenshotting the ncis.navy.mil website on September 19th, 2024. Source: https://urlscan.io/result/559c2119-a238-48e8-b7e9-5ba5d95a529b/

One can use URLScan.io to identify instances where various ad tech vendors served ads to bots. For example, in the screenshot below, one can see a US Navy recruiting ad that was served to URLScan.io's bot on June 16th, 2023, when the bot was scanning msn.com.



www.msn.com

204.79.197.203

Submitted URL: https://www.msn.com/en-us/music/celebrity/these-celebrities-are-not-considered-lgbtq-allies-some-on-this-list-may-su...

Effective URL: https://www.msn.com/en-us/music/celebrity/these-celebrities-are-not-considered-lgbtq-allies-some-on-this-list-may-su...

Submission: On June 16 via manual (June 16th 2023, 3:05:06 pm UTC) from US — Scanned from US

Summary

This website contacted 70 IPs in 7 countries across 55 domains to perform 442 HTTP transactions. The main IP is 204.79.197.203, located in United States and belongs to MICROSOFT-CORP-MSN-AS-BLOCK, US. The main domain is www.msn.com. The Cisco Umbrella rank of the primary domain is 539.
TLS certificate: Issued by *Microsoft RSA TLS CA 01* on September 8th 2022. Valid for: a year.

www.msn.com scanned 10000+ times on urlscan.io

urlscan.io Verdict: No classification ✓

Live information

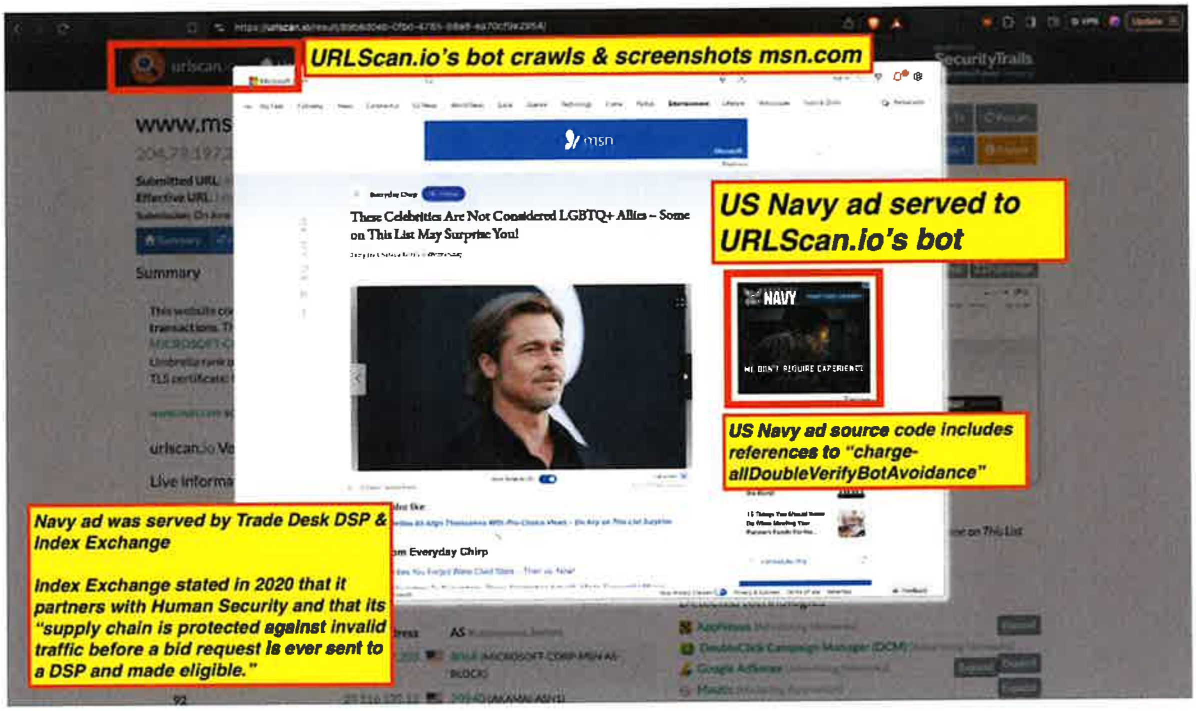
Google Safe Browsing: ✓ No classification for www.msn.com
Current DNS A record: 204.79.197.203 (AS8068 - MICROSOFT-CORP-MSN-AS-BLOCK, US)
Domain created: November 10th 1994, 00:00:00 (UTC)
Domain registrar: MarkMonitor, Inc.

Screenshot

Screenshot of a URLScan.io bot crawl of msn.com on June 16th, 2023, with a US Navy recruiting ad served to the bot. Source: https://urlscan.io/result/89b8d0eb-0fbd-4785-98a8-ea70cf9e2954/

Analyzing the source code of the US Navy ad shows that the ad was transacted by the Trade Desk DSP and Index Exchange SSP (seller ID 185185). The source code of the US Navy ads contains references to "charge-allDoubleVerifyBotAvoidance". Index Exchange and HUMAN Security also has issued public statements that: it has an "*expanded partnership that enhances Index Exchange's global inventory across all channels and regions. Through White Ops' comprehensive protection, **the partnership protects the entirety** of Index Exchange's global inventory. It allows buyers to purchase from IX's emerging channels, such as mobile app and Connected TV (CTV), with confidence that **its supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible***" (emphasis added).

https://adalytics.io/blog/prebid-bot-filtration


urlscan
www.ms
Summary
msn
These Celebrities Are Not Considered LGBTQ+ Allies – Some on This List May Surprise You!
NAVY
WE DON'T REQUIRE EXPERIENCE
SecurityTrails
Everyday Chirp

URLScan.io's bot crawls & screenshots msn.com

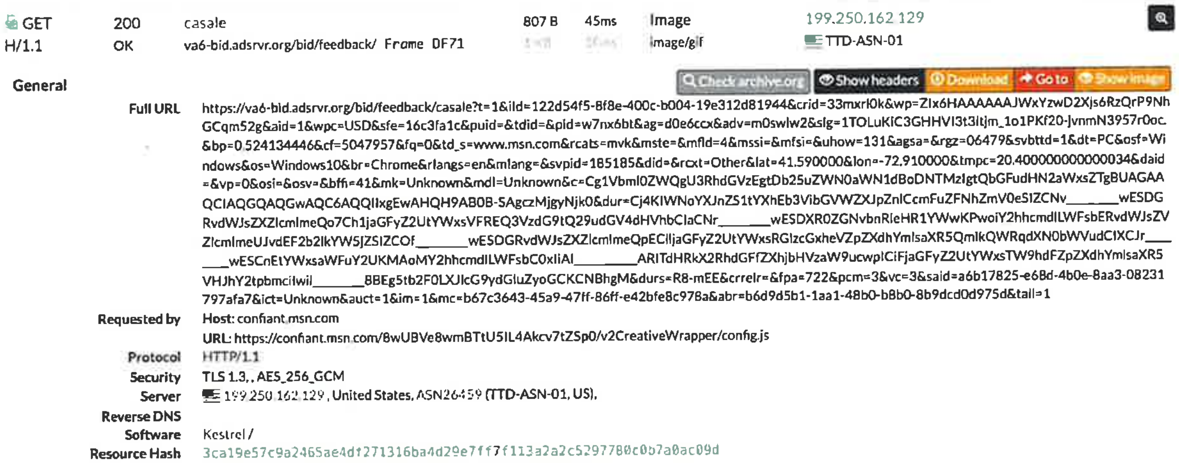
US Navy ad served to URLScan.io's bot

US Navy ad source code includes references to "charge-allDoubleVerifyBotAvoidance"

Navy ad was served by Trade Desk DSP & Index Exchange

Index Exchange stated in 2020 that it partners with Human Security and that its "supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible."

Screenshot of URLScan.io's website, showing a URLScan.io bot crawl from June 16th, 2023. One can see a US Navy ad that was mediated by Trade Desk, Index Exchange, DoubleVerify, and/or HUMAN Security on msn.com.



```
GET     200   casale                                       807 B   45ms   Image        199.250.162.129
H/1.1   OK    va6-bid.adsrvr.org/bid/feedback/  Frame DF71                image/gif    TTD-ASN-01

General

Full URL        https://va6-bid.adsrvr.org/bid/feedback/casale?t=1&iId=122d54f5-8f8e-400c-b004-19e312d81944&crid=33mxrl0k&wp=ZIx6HAAAAAAJWxYzwD2Xjs6RzQrP9Nh
                GCqm52g&aid=1&wpc=USD&sfe=16c3fa1c&puid=&tdid=&pid=w7nx6bt&ag=d0e6ccx&adv=m0swlw2&sig=1TOLuKIC3GHHVI3t3Itjm_1o1PKf20-JvnmN3957r0oc
                &bp=0.524134446&cf=5047957&fq=0&td_s=www.msn.com&rcats=mvk&mste=&mfld=4&mssi=&mfsi=&uhow=131&agsa=&rgz=06479&svbttd=1&dt=PC&osf=Wi
                ndows&os=Windows10&br=Chrome&rlangs=en&mlang=&svpid=185185&did=&rcxt=Other&lat=41.590000&lon=-72.910000&tmpc=20.400000000000034&daid
                =&vp=0&osi=&osv=&bffi=41&mk=Unknown&mdl=Unknown&c=Cg1Vbml0ZWQgU3RhdGVzEgtDb25uZWN0aWN1dBoDNTMzIgtQbGFudHN2aWxsZTgBUAGAA
                QCIAQGQAQGwAQC6AQQIIxgEwAHQH9AB0B-SAgczMjgyNjk0&dur=Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv_______wESDG
                RvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3VzdG9tQ29udGV4dHVhbClaCNr_______wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsbERvdWJsZV
                ZlcmlmeUJvdEF2b2lkYW5jZSIZCOf_______wESDGRvdWJsZXZlcmlmeQpECiljaGFyZ2UtYWxsRGlzcGxheVZpZXdhYmlsaXR5QmlkQWRqdXN0bWVudCIXCJr____
                ____wESCnEtYWxsaWFuY2UKMAoMY2hhcmdlLWFsbC0xliAI_________ARITdHRkX2RhdGFfZXhjbHVzaW9ucwplCiFjaGFyZ2UtYWxsTW9hdFZpZXdhYmlsaXR5
                VHJhY2tpbmcilwil_______8BEg5tb2F0LXJlcG9ydGluZyoGCKCNBhgM&durs=R8-mEE&crrelr=&fpa=722&pcm=3&vc=3&said=a6b17825-e68d-4b0e-8aa3-08231
                797afa7&ict=Unknown&auct=1&im=1&mc=b67c3643-45a9-47ff-86ff-e42bfe8c978a&abr=b6d9d5b1-1aa1-48b0-b8b0-8b9dcd0d975d&tail=1
Requested by    Host: confiant.msn.com
                URL: https://confiant.msn.com/8wUBVe8wmBTtU5IL4Akcv7tZSp0/v2CreativeWrapper/config.js
Protocol        HTTP/1.1
Security        TLS 1.3, , AES_256_GCM
Server          199.250.162.129 , United States, ASN26459 (TTD-ASN-01, US),
Reverse DNS
Software        Kestrel /
Resource Hash   3ca19e57c9a2465ae4df271316ba4d29e7ff7f113a2a2c5297780c0b7a0ac09d
```

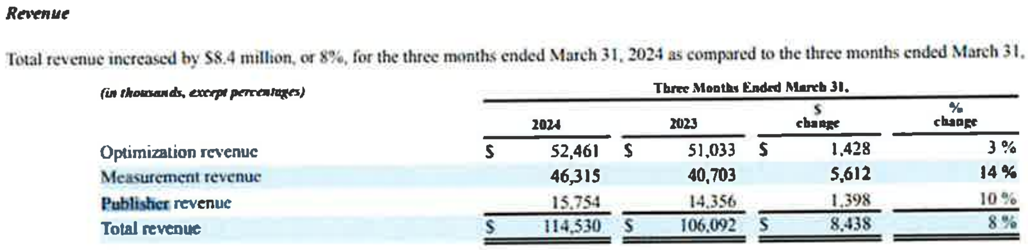
Screenshot of URLScan.io's HTTP requests tab for a URLScan.io bot crawl on June 16th, 2023. The screenshot shows an HTTP request to "bid.adsrv.org/bid/feedback/casale" - a "win notification" pixel that fires when a Trade Desk ad transacts via Index Exchange SSP on msn.com

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Research Methodology - Examination of putative bot traffic classifications from IAS on various sites

In addition to providing services to advertisers, Integral Ad Science (IAS) also accepts financial payments from and provides services to media publishers.

For example, one can see that IAS made $15.7 million dollars in revenue from publishers in Q1 2024, according to IAS's 10-Q form.



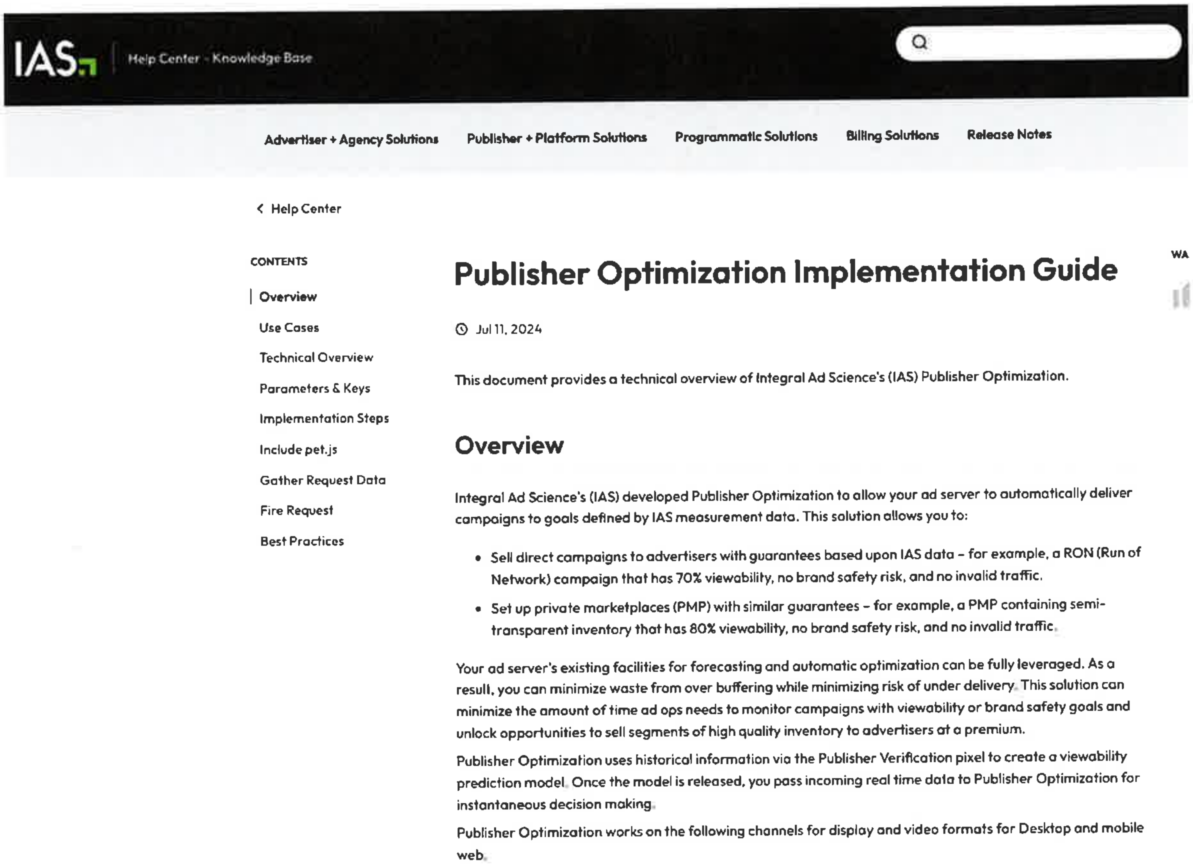
Revenue

Total revenue increased by $8.4 million, or 8%, for the three months ended March 31, 2024 as compared to the three months ended March 31, 2023.

(in thousands, except percentages)	Three Months Ended March 31,			
	2024	2023	$ change	% change
Optimization revenue	$ 52,461	$ 51,033	$ 1,428	3 %
Measurement revenue	46,315	40,703	5,612	14 %
Publisher revenue	15,754	14,356	1,398	10 %
Total revenue	$ 114,530	$ 106,092	$ 8,438	8 %

Screenshot of IAS's Q1 2024 10-Q form, showing that IAS made $15.7 million in revenue providing services to publishers

IAS releases publisher specific tools, some of which appear to be invoked before any ads are served or ad auctions run on a given page. Specifically, IAS's public "publisher optimization implementation guide" provides a technical overview of its publisher tools.



Publisher Optimization Implementation Guide

Jul 11, 2024

This document provides a technical overview of Integral Ad Science's (IAS) Publisher Optimization.

Overview

Integral Ad Science's (IAS) developed Publisher Optimization to allow your ad server to automatically deliver campaigns to goals defined by IAS measurement data. This solution allows you to:

- Sell direct campaigns to advertisers with guarantees based upon IAS data – for example, a RON (Run of Network) campaign that has 70% viewability, no brand safety risk, and no invalid traffic.
- Set up private marketplaces (PMP) with similar guarantees – for example, a PMP containing semi-transparent inventory that has 80% viewability, no brand safety risk, and no invalid traffic.

Your ad server's existing facilities for forecasting and automatic optimization can be fully leveraged. As a result, you can minimize waste from over buffering while minimizing risk of under delivery. This solution can minimize the amount of time ad ops needs to monitor campaigns with viewability or brand safety goals and unlock opportunities to sell segments of high quality inventory to advertisers at a premium.

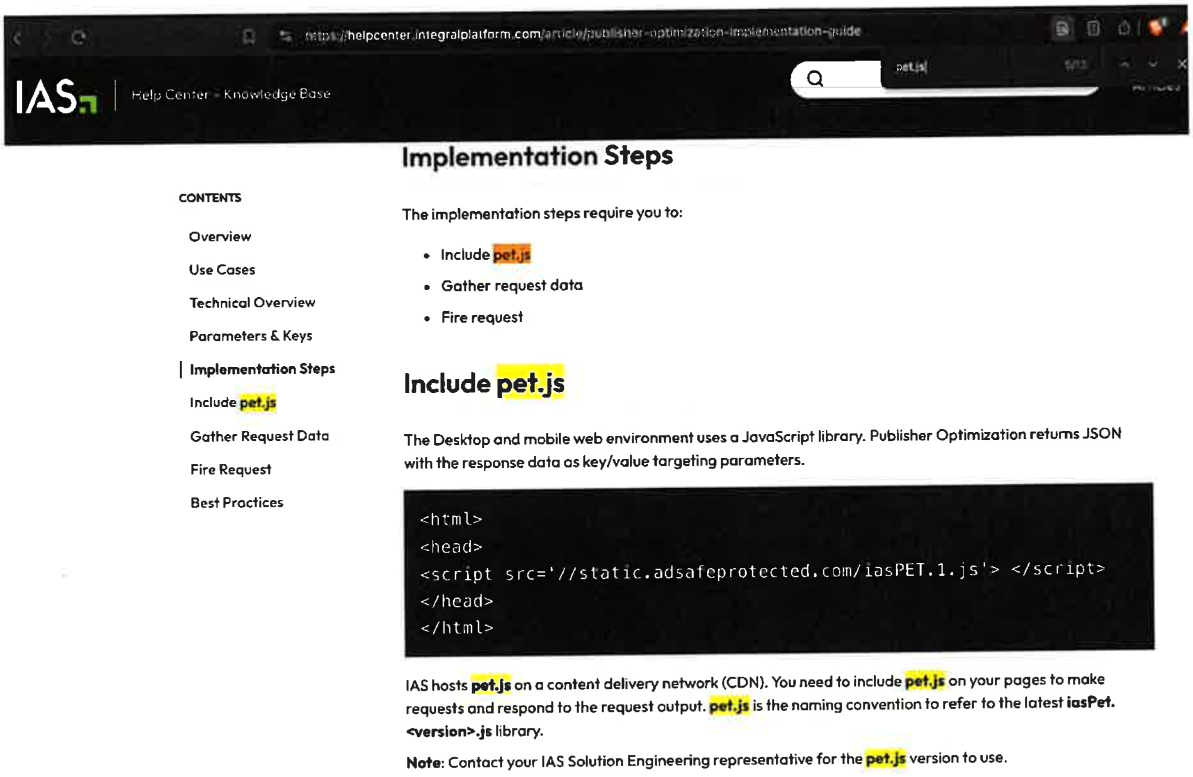
Publisher Optimization uses historical information via the Publisher Verification pixel to create a viewability prediction model. Once the model is released, you pass incoming real time data to Publisher Optimization for instantaneous decision making.

Publisher Optimization works on the following channels for display and video formats for Desktop and mobile web.

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link: https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

IAS's public "Publisher Optimization Implementation Guide" explains that the "The desktop and mobile web environment uses a JavaScript library. Publisher Optimization returns JSON with the response data as key/value targeting parameters." This is loaded via a specific Javascript file called: "static.adsafeprotected.com/iasPET.1.js".

https://adalytics.io/blog/prebid-bot-filtration


https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide
IAS
Help Center - Knowledge Base
pet.js

Implementation Steps

CONTENTS

- Overview
- Use Cases
- Technical Overview
- Parameters & Keys
- Implementation Steps
- Include pet.js
- Gather Request Data
- Fire Request
- Best Practices

The implementation steps require you to:

- Include pet.js
- Gather request data
- Fire request

Include pet.js

The Desktop and mobile web environment uses a JavaScript library. Publisher Optimization returns JSON with the response data as key/value targeting parameters.

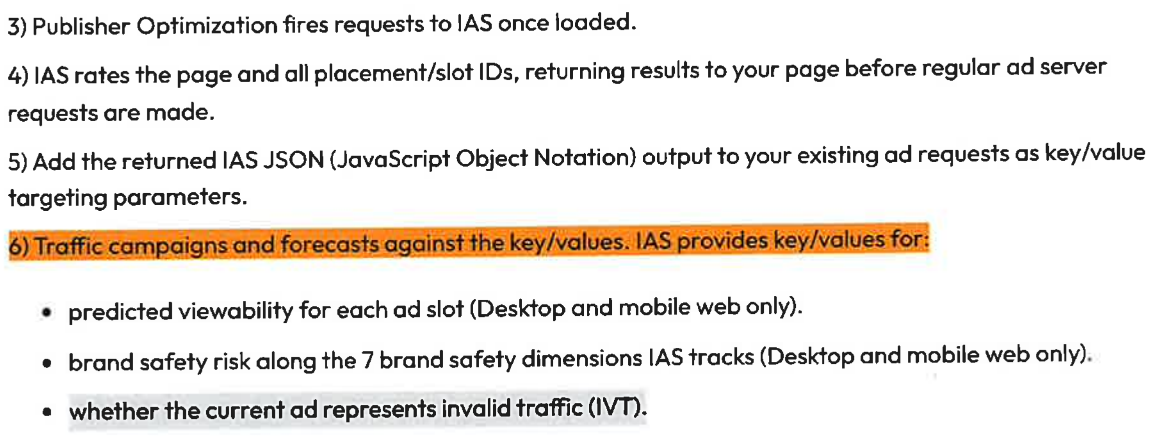
```
<html>
<head>
<script src='//static.adsafeprotected.com/iasPET.1.js'> </script>
</head>
</html>
```

IAS hosts pet.js on a content delivery network (CDN). You need to include pet.js on your pages to make requests and respond to the request output. pet.js is the naming convention to refer to the latest **iasPet.<version>.js** library.

Note: Contact your IAS Solution Engineering representative for the pet.js version to use.

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide"

The IAS Publisher Optimization tool "provides key/values for: [...] whether the current ad represents invalid traffic (IVT)."



3) Publisher Optimization fires requests to IAS once loaded.

4) IAS rates the page and all placement/slot IDs, returning results to your page before regular ad server requests are made.

5) Add the returned IAS JSON (JavaScript Object Notation) output to your existing ad requests as key/value targeting parameters.

6) Traffic campaigns and forecasts against the key/values. IAS provides key/values for:

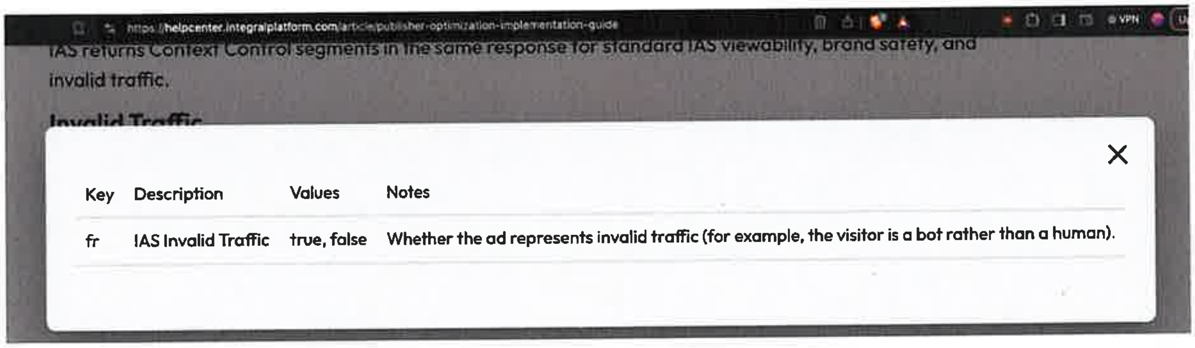
- predicted viewability for each ad slot (Desktop and mobile web only).
- brand safety risk along the 7 brand safety dimensions IAS tracks (Desktop and mobile web only).
- whether the current ad represents invalid traffic (IVT).

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link:

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

IAS's "publisher optimization implementation guide" reveals that the vendor uses the "fr" key to indicate "IAS Invalid Traffic". Possible values for the "fr" key include "fr=true" or "fr=false. The guide explains that this indicates "Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human)." "fr=true" represents the user is classified as a "bot", whilst "fr=false" represents the user is classified as a human.


https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide
VPN

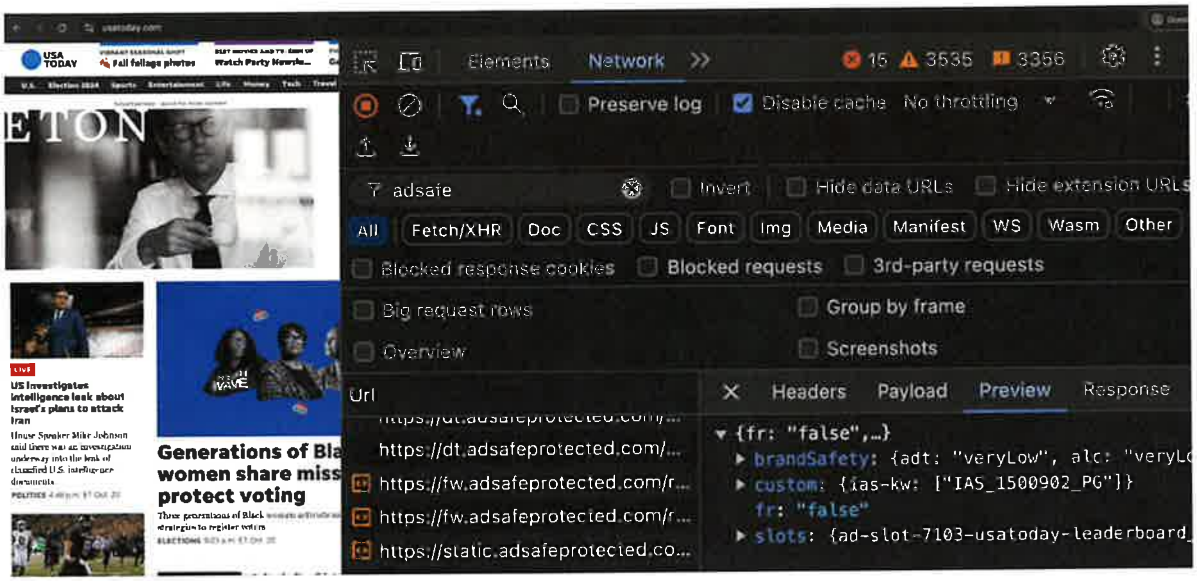
IAS returns Context Control segments in the same response for standard IAS viewability, brand safety, and invalid traffic.

Invalid Traffic

Key	Description	Values	Notes
fr	IAS Invalid Traffic	true, false	Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human).

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link: https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

In the screenshot below, one can see an example of IAS's publisher optimization tools returning an HTTP response from the endpoint "pixel.adsafeprotected.com/services/pub", wherein the "fr" value is set to "fr=false".



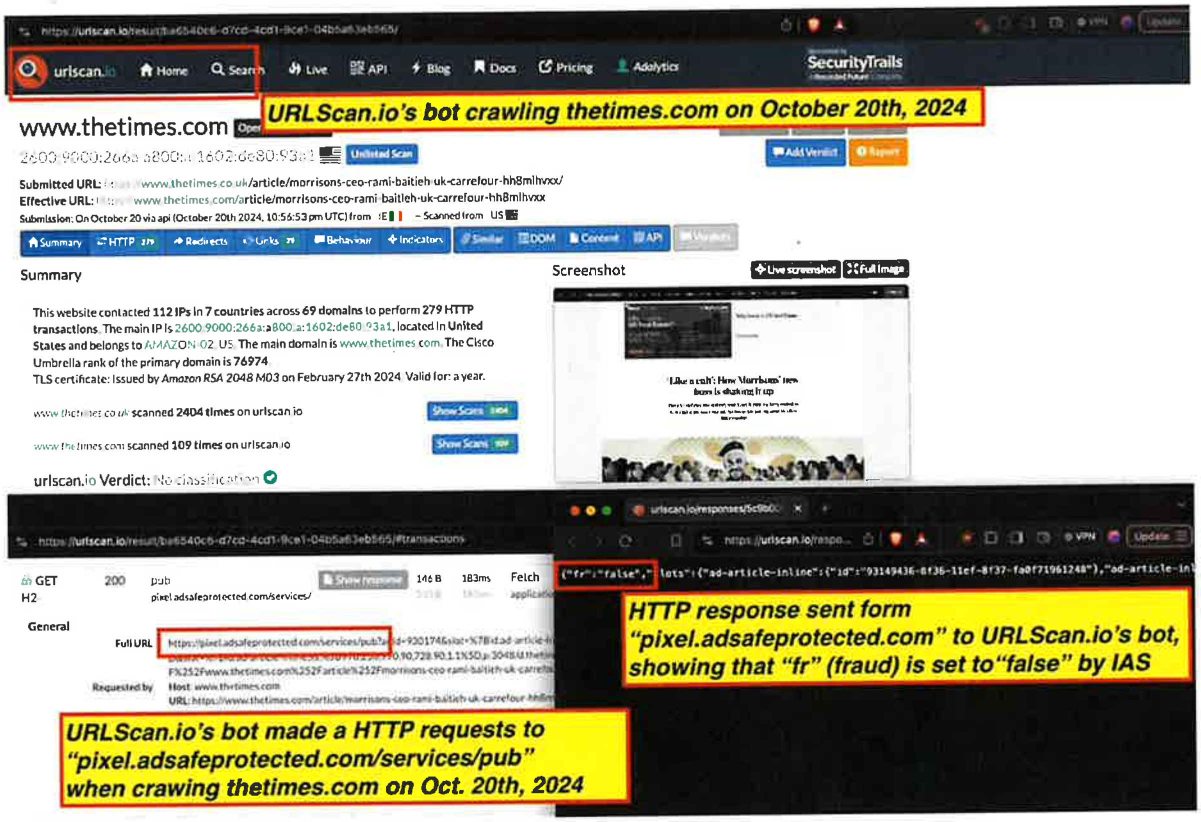
```
https://dt.adsafeprotected.com/...
https://dt.adsafeprotected.com/...
https://fw.adsafeprotected.com/r...
https://fw.adsafeprotected.com/r...
https://static.adsafeprotected.co...
```

```
▾ {fr: "false",…}
  ▸ brandSafety: {adt: "veryLow", alc: "veryLo
  ▸ custom: {ias-kw: ["IAS_1500902_PG"]}
    fr: "false"
  ▸ slots: {ad-slot-7103-usatoday-leaderboard_
```

Screenshot of chrome developer tools, showing that "fr: false" in the lower right hand corner, for IAS's endpoint "pixel.adsafeprotected.com/services/pub" on usatoday.com.

Given a sample dataset of 100% confirmed bot traffic as a ground truth baseline, one can perform a calibration exercise to statistically estimate the statistical sensitivity ("True Positive Rate") of the IAS publisher optimization software for detecting bot traffic.

For example, for a set of bot crawls, one can see whether IAS's "pixel.adsafeprotected.com" endpoint returned a value of "fr=true" or "fr=false". In the screenshot below, one can see an instance where URLScan.io's bot crawled thetimes.com on October 20th, 2024. One can see that, when the bot was crawling thetimes.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false".



URLScan.io's bot crawling thetimes.com on October 20th, 2024

www.thetimes.com

2600:9000:266a:a800:a:1602:de80:93a1

Submitted URL: https://www.thetimes.co.uk/article/morrisons-ceo-rami-baitieh-uk-carrefour-hh8mlhvxx/
Effective URL: https://www.thetimes.com/article/morrisons-ceo-rami-baitieh-uk-carrefour-hh8mlhvxx
Submission: On October 20 via api (October 20th 2024, 10:56:53 pm UTC) from IE — Scanned from US

Summary

This website contacted 112 IPs in 7 countries across 69 domains to perform 279 HTTP transactions. The main IP is 2600:9000:266a:a800:a:1602:de80:93a1, located in United States and belongs to AMAZON-02, US. The main domain is www.thetimes.com. The Cisco Umbrella rank of the primary domain is 76974.
TLS certificate: Issued by Amazon RSA 2048 M03 on February 27th 2024. Valid for: a year.

www.thetimes.co.uk scanned 2404 times on urlscan.io

www.thetimes.com scanned 109 times on urlscan.io

urlscan.io Verdict: No classification

```
GET   200   pub                              146 B   183ms   Fetch
H2          pixel.adsafeprotected.com/services/                   applicatio
```

General

Full URL: https://pixel.adsafeprotected.com/services/pub?a...id=9201746slot=%7B...ad-article-i...
...0,90,728,90,1,1%5D...p:3048...
F%252Fwww.thetimes.com%252Farticle%252Fmorrisons-ceo-rami-baitieh-uk-carrefo...

Requested by: Host: www.thetimes.com
URL: https://www.thetimes.com/article/morrisons-ceo-rami-baitieh-uk-carrefour-hh8m...

```
{"fr":"false","slots":{"ad-article-inline":{"id":"93149436-8f36-11ef-8f37-fa0f71961248"},"ad-article-in
```

HTTP response sent form "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to"false" by IAS

URLScan.io's bot made a HTTP requests to "pixel.adsafeprotected.com/services/pub" when crawing thetimes.com on Oct. 20th, 2024

Composite screenshot of URLScan.io's bot crawling thetimes.com on October 20th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false".

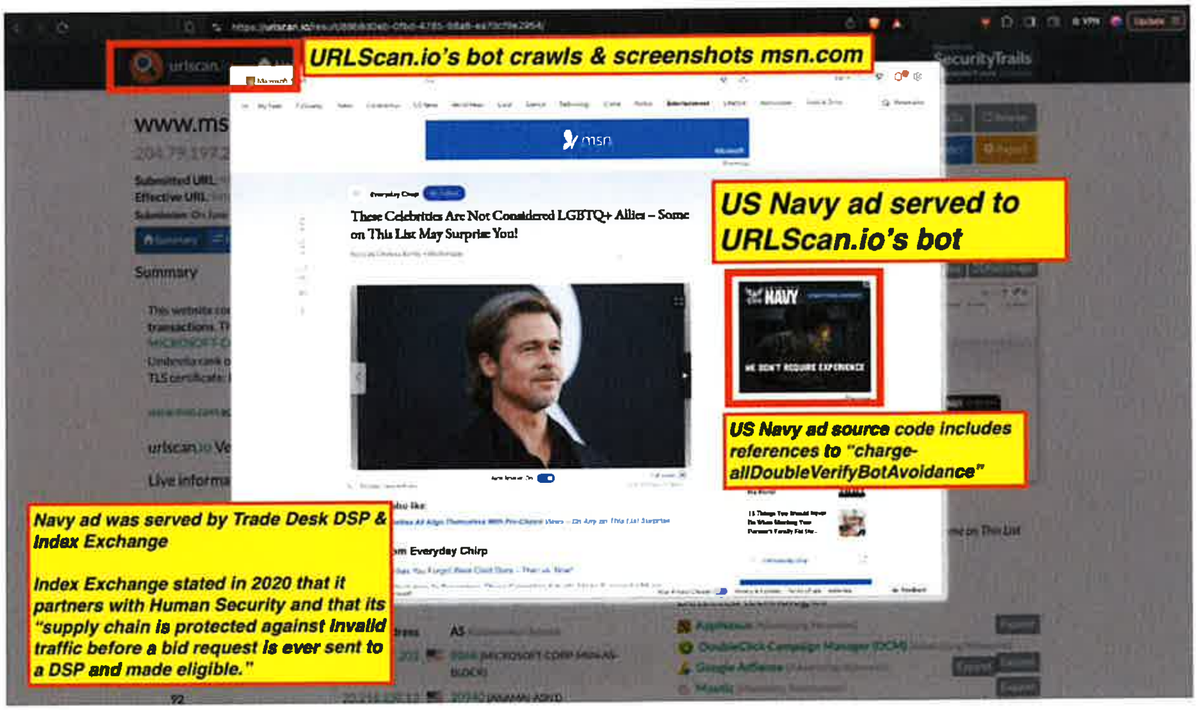
Research Methodology - Digital forensics of ad source code

When an ad is served to a bot in a data center and recorded by the bot (in the form of an HTTP network traffic logfile), one can inspect the source code of the HTTP requests and resources used to serve the ad to the given bot.

Analyzing source code of digital ads allows one to identify which Supply Side Platforms (SSPs) or ad exchanges were involved in transacting a given ad. For example, if an ad was served via the TripleLift header bidding adapter or contained an image pixel whose "src" (source) attribute was the endpoint "tlx.3lift.com/s2s/notify" or "tlx.3lift.com/header/notify", the given ad was labeled as having been transacted by TripleLift ad exchange. Similarly, if an ad was served contained an image pixel whose "src" attribute was the endpoint "bid.adsrvr.org/bid/feedback" or "us-east-1.event.prod.bidr.io/log/imp/", the given ad was was labeled as having been transacted by Trade Desk or Beeswax DSP, respectively.

For a subset of digital ads observed, it appears to be possible to extract from the source code of the ad if a given brand appeared to be "charged" (invoiced) for bot avoidance or page quality services from a given vendor. The source of some ads appear to contain (in Base64 encoded text) references to specific data segments, vendors, or services that were applied for a given ad campaign.

For example, many US Navy ads observed being served to bots in data centers contained Javascript from doubleverify.com and source code from a demand side platform, which included Base64 encoded text. For example, in the screenshot below, one can see a US Navy ad served to a bot that was crawling msn.com (source: https://urlscan.io/result/89b8d0eb-0fbd-4785-98a8-ea70cf9e2954/#summary).



URLScan.io's bot crawls & screenshots msn.com

US Navy ad served to URLScan.io's bot

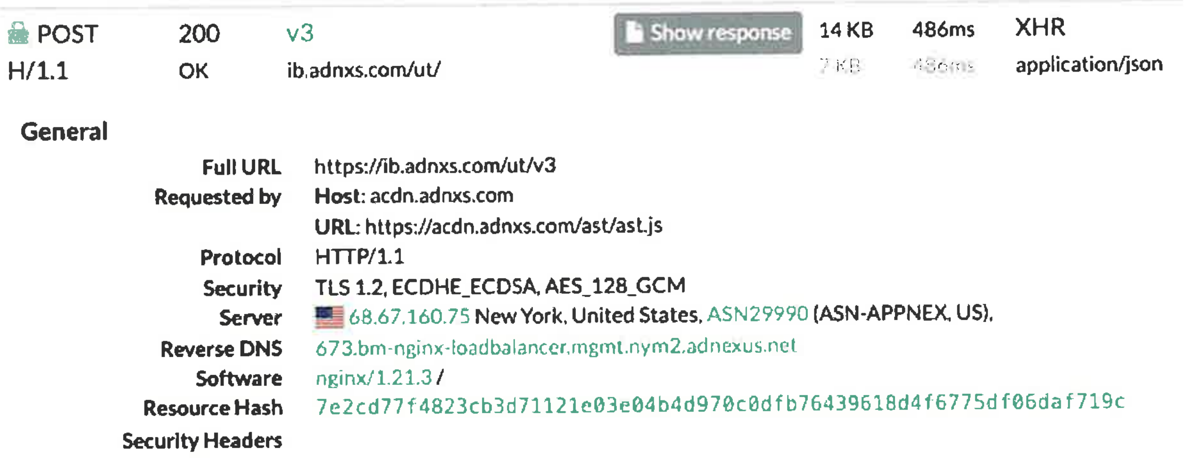
US Navy ad source code includes references to "charge-allDoubleVerifyBotAvoidance"

Navy ad was served by Trade Desk DSP & Index Exchange

Index Exchange stated in 2020 that it partners with Human Security and that its "supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible."

urlscan
www.ms
msn
These Celebrities Are Not Considered LGBTQ+ Allies – Some on This List May Surprise You!
NAVY
WE DON'T REQUIRE EXPERIENCE
SecurityTrails
Everyday Chirp
MICROSOFT-CORP-MSN-AS-BLOCK
DoubleClick Campaign Manager (DCM)

Inspecting the source code of the HTTP traffic that served the ad shows that the bid response was served via Microsoft Xandr's (formerly known as AppNexus) Prebid server via the endpoint: https://ib.adnxs.com/ut/v3.

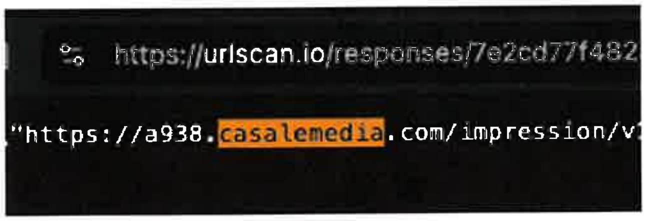

POST H/1.1 200 OK v3 ib.adnxs.com/ut/ Show response 14 KB 7 KB 486ms 486ms XHR application/json

General

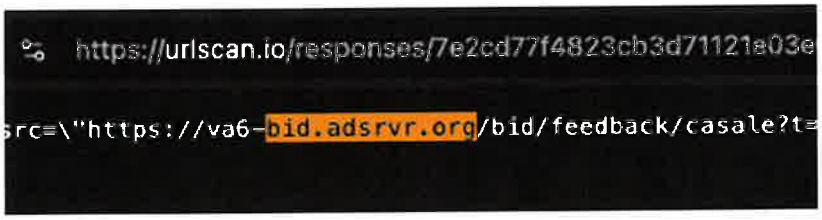
Full URL https://ib.adnxs.com/ut/v3
Requested by Host: acdn.adnxs.com
URL: https://acdn.adnxs.com/ast/ast.js
Protocol HTTP/1.1
Security TLS 1.2, ECDHE_ECDSA, AES_128_GCM
Server 68.67.160.75 New York, United States, ASN29990 (ASN-APPNEX, US),
Reverse DNS 673.bm-nginx-loadbalancer.mgmt.nym2.adnexus.net
Software nginx/1.21.3 /
Resource Hash 7e2cd77f4823cb3d71121e03e04b4d970c0dfb76439618d4f6775df06daf719c
Security Headers

Screenshot from URLScan.io showing the individual HTTP POST request that served the US Navy ad to a bot. Source: https://urlscan.io/result/89b8d0eb-0fbd-4785-98a8-ea70cf9e2954/#transactions

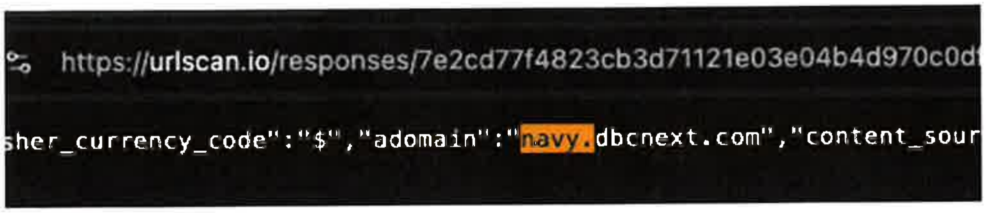
One can inspect the HTTP response from Microsoft Xandr's Prebid server to see that the bid response was transacted by Index Exchange supply side platform (which owns the domain casalemedia.com) and by the demand side platform Trade Desk.


https://urlscan.io/responses/7e2cd77f482

```
"https://a938.casalemedia.com/impression/v
```


https://urlscan.io/responses/7e2cd77f4823cb3d71121e03e

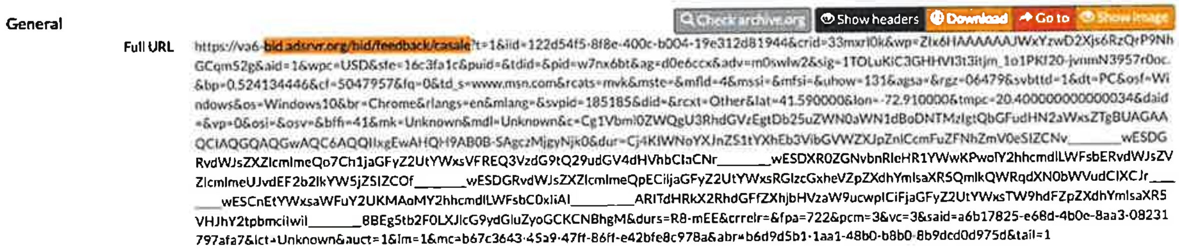
```
src=\"https://va6-bid.adsrvr.org/bid/feedback/casale?t=
```



```
https://urlscan.io/responses/7e2cd77f4823cb3d71121e03e04b4d970c0d
her_currency_code":"$","adomain":"navy.dbcnext.com","content_sour
```

Screenshots of source code of an HTTP bid response from Microsoft Xandr's Prebid server, when serving a US Navy ad to a bot. Source: https://urlscan.io/responses/7e2cd77f4823cb3d71121e03e04b4d970c0dfb76439618d4f6775df06daf719c/

One can carefully analyze the Trade Desk demand side platform win notification pixel that was triggered when the US Navy ad was served to the bot.



General

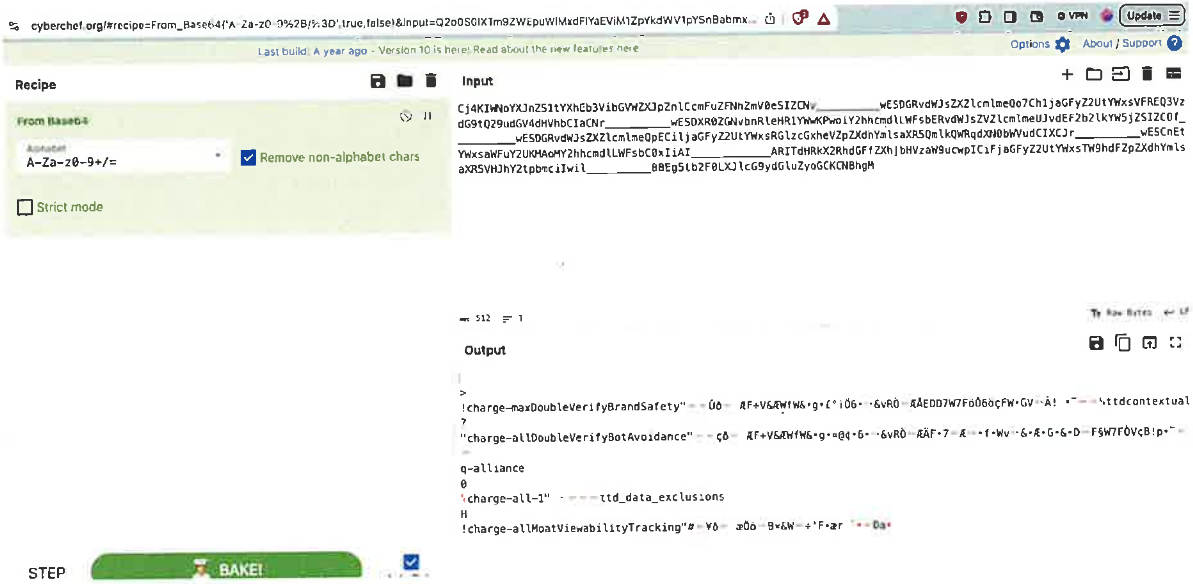
Full URL

```
https://va6-bid.adsrvr.org/bid/feedback/casale?t=1&iid=122d54f5-8f8e-400c-b004-19e312d81944&crid=33mxrl0k&wp=ZIk6HAAAAAAJWxYzwD2Xjs6RzQrP9Nh
GCqm52g&aid=1&wpc=USD&sfe=16c3fa1c&puid=&tdid=&pid=w7nx6bt&ag=d0e6ccx&adv=m0swlw2&sig=1TOLuKiC3GHHVI3t3itjm_1o1PKf20-jvmmN3957r0oc.
&bp=0.524134446&cf=5047957&fq=0&td_s=www.msn.com&rcats=mvk&mste=&mfld=4&mssi=&mfsi=&uhow=131&agsa=&rgz=06479&svbttd=1&dt=PC&osf=Wi
ndows&os=Windows10&br=Chrome&rlangs=en&mlang=&svpid=185185&did=&rcxt=Other&lat=41.590000&lon=-72.910000&tmpc=20.400000000000034&daid
=&vp=0&osi=&osv=&bffi=41&mk=Unknown&mdl=Unknown&c=Cg1Vbml0ZWQgU3RhdGVzEgtDb25uZWN0aWN1dBoDNTMzIgtQbGFudHN2aWxsZTgBUAGAA
QCIAQGQAQGwAQC6AQQIIxgEwAHQH9AB0B-SAgczMjgyNjk0&dur=Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv________wESDG
RvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3VzdG9tQ29udGV4dHVhbCIaCNr________wESDXR0ZGNvbnRleHR1YWwKPwoIY2hhcmdlLWFsbERvdWJsZV
ZlcmlmeUJvdEF2b2lkYW5jZSIZCOf________wESDGRvdWJsZXZlcmlmeQpECiljaGFyZ2UtYWxsRGlzcGxheVZpZXdhYmlsaXR5QmlkQWRqdXN0bWVudCIXCJr___
____wESCnEtYWxsaWFuY2UKMAoMY2hhcmdlLWFsbC0xliAI_________ARITdHRkX2RhdGFfZXhjbHVzaW9ucwplCiFjaGFyZ2UtYWxsTW9hdFZpZXdhYmlsaXR5
VHJhY2tpbmcilwil________8BEg5tb2F0LXJlcG9ydGluZyoGCKCNBhgM&durs=R8-mEE&crrelr=&fpa=722&pcm=3&vc=3&said=a6b17825-e68d-4b0e-8aa3-08231
797afa7&lct=Unknown&auct=1&lm=1&mc=b67c3643-45a9-47ff-86f1-e42bfe8c978a&abr=b6d9d5b1-1aa1-48b0-b8b0-8b9dcd0d975d&tail=1
```

The US Navy ad includes a DSP win notification pixel with the "dur=" query string parameter.

The value of the "dur=" query string parameter from the US Navy DSP win notification pixel is a base64 encoded string: "Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv_________wESDGRvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3VzdG9tQ29udGV4dHVhbCIaCNr_________wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsbERvdWJsZVZlcmlmeUJvdEF2b2lkYW5jZSIZCOf_________wESDGRvdWJsZXZlcmlmeQpECiljaGFyZ2UtYWxsRGlzcGxheVZpZXdhYmlsaXR5QmlkQWRqdXN0bWVudCIXCJr_________wESCnEtYWxsaWFuY2UKMAoMY2hhcmdlLWFsbC0xliAI___________ARITdHRkX2RhdGFfZXhjbHVzaW9ucwplCiFjaGFyZ2UtYWxsTW9hdFZpZXdhYmlsaXR5VHJhY2tpbmcilwil_________8BEg5tb2F0LXJlcG9ydGluZyoGCKCNBhgM".

If one copies that specific "dur=" query string parameter and opens the website cyberchef.org (an online web utility or tool provided by the UK signals intelligence agency GCHQ that helps Base64 decode text), one can see the decoded value of this specific “dur=” query string parameter. cyberchef.org shows that the decoded value of the “dur=” query string parameter from the Ikea ad contains references to “charge-allDoubleVerifyBotAvoidance”.



cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Q2o0S0lXTm9ZWEpuWlMxdFlYaEViM1ZpYkdWV1pYSnBabmx...

Last build: A year ago - Version 10 is here! Read about the new features here

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input

Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCN__________wESDGRvdWJsZXZlcmlmeQo7ChljaGFyZ2UtYWxsVFREQ3Vz
dG9tQ29udGV4dHVhbCIaCNr__________wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsbERvdWJsZVZlcmlmeUJvdEF2b2lkYW5jZSIZCOf_
__________wESDGRvdWJsZXZlcmlmeQpECiljaGFyZ2UtYWxsRGlzcGxheVZpZXdhYmlsaXR5QmlkQWRqdXN0bWVudCIXCJr__________wESCnEt
YWxsaWFuY2UKMAoMY2hhcmdlLWFsbC0xIiAI_____________ARITdHRkX2RhdGFfZXhjbHVzaW9ucwpICiFjaGFyZ2UtYWxsTW9hdFZpZXdhYmls
aXR5VHJhY2tpbmciIwil___________BBEgStb2F0LXJlcG9ydGluZyoGCKCNBhgM

512 1

Output

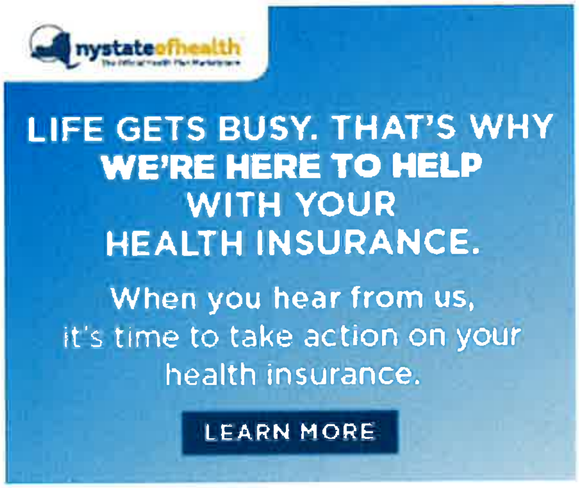
```
>
!charge-maxDoubleVerifyBrandSafety"  Ûð  ÆF+V&ÆWfW&•g•£°iÖ6• •&vRÒ ÆÄEDD7W7FöÖ6öçFW•GV Ä! •¯  \ttdcontextual
?
"charge-allDoubleVerifyBotAvoidance"  çð  ÆF+V&ÆWfW&•g••@¢•6• •&vRÒ ÆÄF•7 Æ •f•Wv •&•Æ•G•&•D F§W7FÖVçB!p•¯
q-alliance
0
\charge-all-1"  ttd_data_exclusions
H
!charge-allMoatViewabilityTracking"#  Yð  æÖö B×&W ÷'F•ær  Da•
```

STEP BAKE!

Screenshot of the website cyberchef.org, with the “dur=” query string parameter text from the same US Navy ad that was served to a bot inputted, and the Base64 decoded text in the lower part of the screen. In the lower part of the screenshot, one can observe a reference to “charge-allDoubleVerifyBotAvoidance”. Full link: https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Q2o0S0lXTm9ZWEpuWlMxdFlYaEViM1ZpYkdWV1pYSnBabmxDY21GdVpGTmhabVYwZVNJWkNOdl9fX19fX19fX193RVNER1J2ZFdKc1pYWmxjbWxtZVFvN0NoMWphR0Z5WjJVdFlXeHNWRVJFUTNWemRHOXRRMjl1ZEdWNGRIVmhiQ0lhQ05yX19fX19fX19fX3dFU0RYUjBaR052Ym5SbGVIUjFZV3dLUHdvaVkyaGhjbWRsTFdGc2JFUnZkV0pzWlZabGNtbG1lVUp2ZEVGMmIybGtZVzVqWlNJWkNPZl9fX19fX19fX193RVNER1J2ZFdKc1pYWmxjbWxtZVFwRUNpbGphR0Z5WjJVdFlXeHNSR2x6Y0d4aGVWWnBaWGRoWW1sc2FYUjVRbWxrUVdScWRYTjBiV1Z1ZENJWENKcl9fX19fX19fX193RVNDbkV0WVd4c2FXRnVZMlVLTUFvTVkyaGhjbWRsTFdGc2JDMHhJaUFJX19fX19fX19fX19fQVJJVGRHUmtYMlJoZEdGZlpYaGpiSFZ6YVc5dWN3cElDaUZqYUdGeVoyVXRZV3hzVFc5aGRGWnBaWGRoWW1sc2FYUjVWSEpoWTJ0cGJtY2lJd2lsX19fX19fX19fX0JCRWdTdGIyRjBMWEpsY0c5eWRHbHVaeW9HQ0tDTkJoZ00

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands’ digital ads to bots?

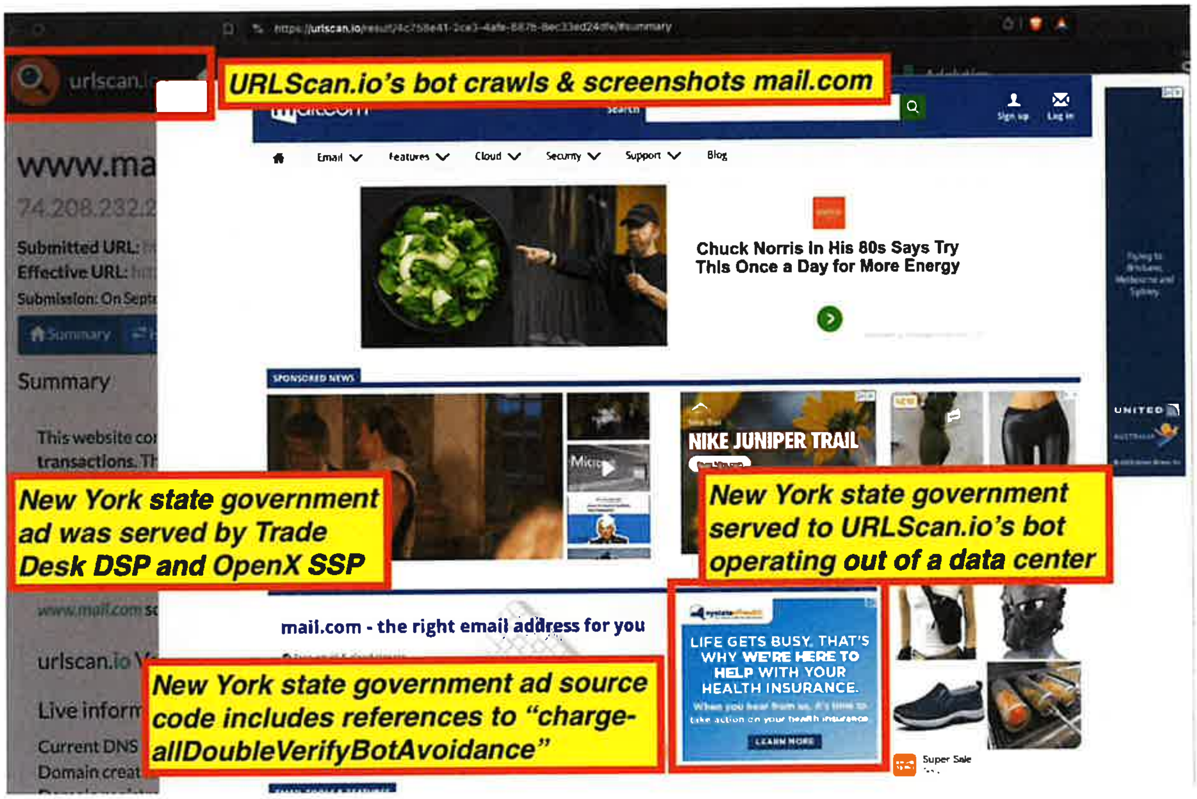
As another example, New York state government (nystateofhealth.ny.gov) ads were observed being served to bots operating out of data centers. Many of the New York state government ads observed being served to bots in data centers contained Javascript from doubleverify.com and source code from a demand side platform, which included Base64 encoded text.


nystateofhealth
LIFE GETS BUSY. THAT'S WHY WE'RE HERE TO HELP WITH YOUR HEALTH INSURANCE.
When you hear from us, it's time to take action on your health insurance.
LEARN MORE

Screenshot of a New York state government ad creative that was served to a bot operating out of a data center by Trade Desk and OpenX. The source code of the New York state government ad contains base64 encoded references to: "charge-allDoubleVerifyBotAvoidance"

For example, a New York state government ad served was served to a bot that was crawling mail.com (source: https://urlscan.io/result/4c758e41-2ce3-4afe-8875-8ec33ed24dfe/#summary). The URLScan.io bot was operating out of an M247 data center when it was served the New York state government ad. The ad was transacted by Trade Desk and OpenX SSP.

https://adalytics.io/blog/prebid-bot-filtration



URLScan.io's bot crawls & screenshots mail.com

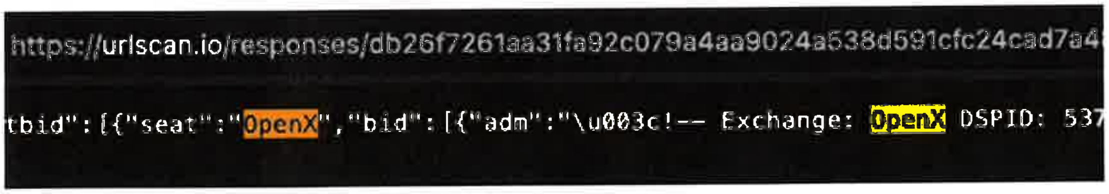
New York state government ad was served by Trade Desk DSP and OpenX SSP

New York state government served to URLScan.io's bot operating out of a data center

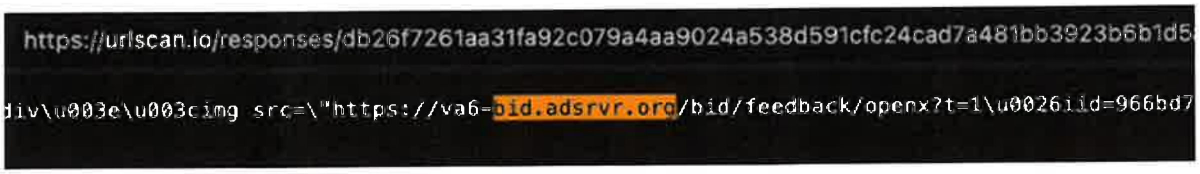
New York state government ad source code includes references to "charge-allDoubleVerifyBotAvoidance"

URLScan.io bot screenshot generated when the bot was operating out of a data center and crawling mail.com. The bot was served a New York state government ad by the Trade Desk and OpenX SSP. The source code of the New York state government ad includes base64 encoded references to "charge-allDoubleVerifyBotAvoidance"

One can inspect the HTTP response from OpenX's server to see that the bid response was transacted by OpenX supply side platform (which owns the domain openx.net) and by the demand side platform Trade Desk.

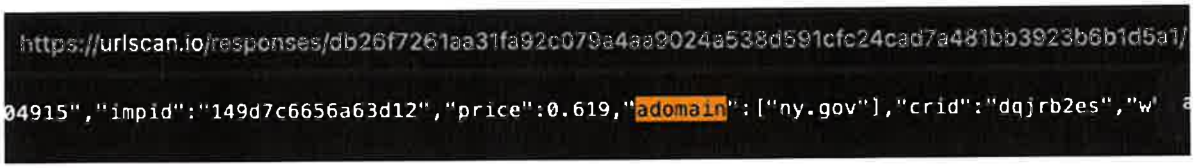


```
https://urlscan.io/responses/db26f7261aa31fa92c079a4aa9024a538d591cfc24cad7a4

tbid":[{"seat":"OpenX","bid":[{"adm":"\u003c!-- Exchange: OpenX DSPID: 537
```



```
https://urlscan.io/responses/db26f7261aa31fa92c079a4aa9024a538d591cfc24cad7a481bb3923b6b1d5

div\u003e\u003cimg src=\"https://va6-bid.adsrvr.org/bid/feedback/openx?t=1\u0026iid=966bd7
```

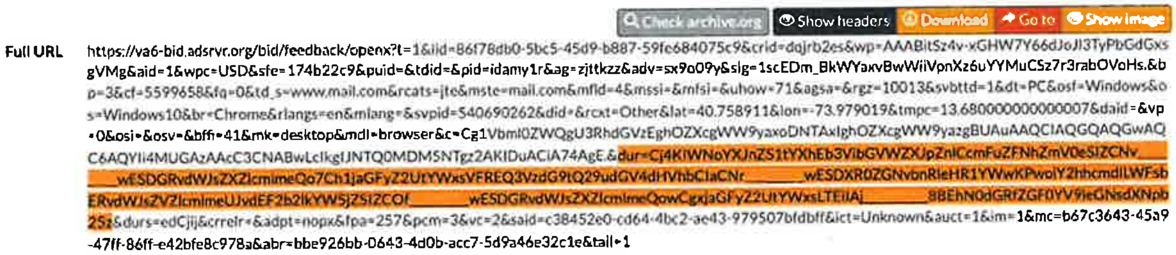
On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?



```
https://urlscan.io/responses/db26f7261aa31fa92c079a4aa9024a538d591cfc24cad7a481bb3923b6b1d5a1/
04915","impid":"149d7c6656a63d12","price":0.619,"adomain":["ny.gov"],"crid":"dqjrb2es","w"
```

Screenshots of source code of an HTTP bid response from OpenX's prebid endpoint, when serving a New York state government ad to a bot in a data center. Source: https://urlscan.io/responses/db26f7261aa31fa92c079a4aa9024a538d591cfc24cad7a481bb3923b6b1d5a1/

One can carefully analyze the Trade Desk demand side platform win notification pixel that was triggered when the New York state government ad was served to the bot operating out of the M247 data center.



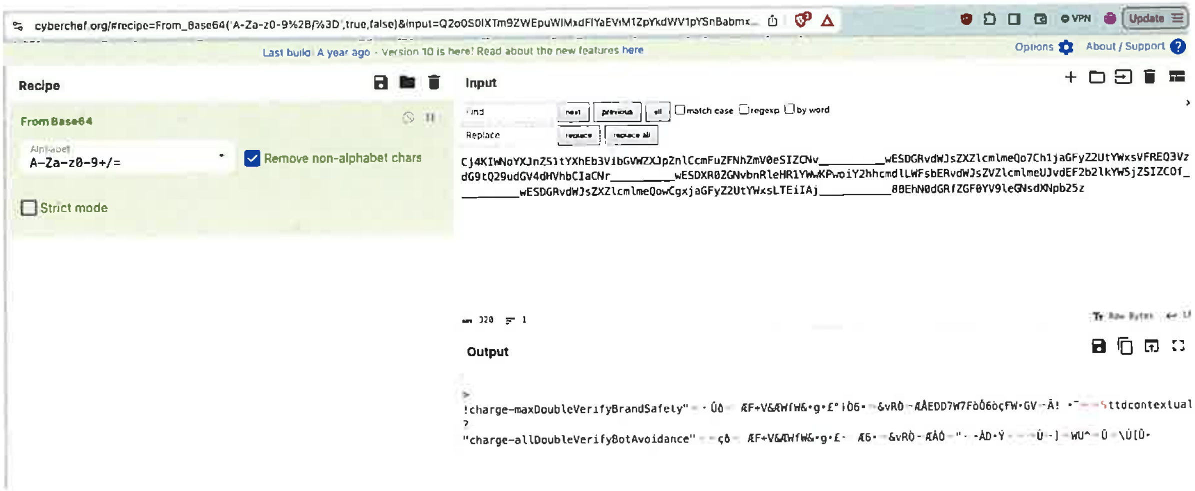
Full URL

```
https://va6-bid.adsrvr.org/bid/feedback/openx?t=1&iid=86f78db0-5bc5-45d9-b887-59fe684075c9&crid=dqjrb2es&wp=AAABitSz4v-xGHW7Y66dJoJl3TyPbGdGxs
gVMg&aid=1&wpc=USD&sfe=174b22c9&puid=&tdid=&pid=idamy1r&ag=zjttkzz&adv=sx9o09y&sig=1scEDm_BkWYaxvBwWilVpnXz6uYYMuCSz7r3rabOVoHs.&b
p=3&cf=5599658&fq=0&td_s=www.mail.com&rcats=jte&mste=mail.com&mfld=4&mssi=&mfsi=&uhow=71&agsa=&rgz=10013&svbttd=1&dt=PC&osf=Windows&o
s=Windows10&br=Chrome&rlangs=en&mlang=&svpid=540690262&did=&rcxt=Other&lat=40.758911&lon=-73.979019&tmpc=13.680000000000007&daid=&vp
=0&osi=&osv=&bffi=41&mk=desktop&mdl=browser&c=Cg1VbmI0ZWQgU3RhdGVzEghOZXcgWW9yaxoDNTAxIghOZXcgWW9yazgBUAuAAQCIAQGQAQGwAQ
C6AQYIi4MUGAzAAcC3CNABwLclkgIJNTQ0MDM5NTgz2AKIDuACiA74AgE.&dur=Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv____
____wESDGRvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3VzdG9tQ29udGV4dHVhbClaCNr________wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsb
ERvdWJsZVZlcmlmeUJvdEF2b2lkYW5jZSIZCOf________wESDGRvdWJsZXZlcmlmeQowCgxjaGFyZ2UtYWxsLTEiIAj__________8BEhN0dGRfZGF0YV9leGNsdXNpb
25z&durs=edCjij&crrelr=&adpt=nopx&fpa=257&pcm=3&vc=2&said=c38452e0-cd64-4bc2-ae43-979507bfdbff&ict=Unknown&auct=1&im=1&mc=b67c3643-45a9
-47ff-86ff-e42bfe8c978a&abr=bbe926bb-0643-4d0b-acc7-5d9a46e32c1e&tall=1
```

The New York state government ad includes a DSP win notification pixel with the "dur=" query string parameter.

The value of the "dur=" query string parameter from the US Navy DSP win notification pixel is a base64 encoded string: "Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv__________wESDGRvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3VzdG9tQ29udGV4dHVhbClaCNr_________wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsbERvdWJsZVZlcmlmeUJvdEF2b2lkYW5jZSIZCOf__________wESDGRvdWJsZXZlcmlmeQowCgxjaGFyZ2UtYWxsLTEiIAj__________8BEhN0dGRfZGF0YV9leGNsdXNpb25z".

If one copies that specific "dur=" query string parameter and opens the website cyberchef.org (an online web utility or tool provided by the UK's signal intelligence agency GCHQ that helps Base64 decode text), one can see the decoded value of this specific "dur=" query string parameter. cyberchef.org shows that the decoded value of the "dur=" query string parameter from the Ikea ad contains references to "charge-allDoubleVerifyBotAvoidance".


cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Q2o0S0lXTm9ZWEpuWlMxdFlYaEViM1ZpYkdWV1pYSnBabmx...

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

□ match case □ regexp □ by word

```
Cj4KIWNoYXJnZS1tYXhEb3VibGVWZXJpZnlCcmFuZFNhZmV0eSIZCNv__________wESDGRvdWJsZXZlcmlmeQo7Ch1jaGFyZ2UtYWxsVFREQ3Vz
dG9tQ29udGV4dHVhbCIaCNr__________wESDXR0ZGNvbnRleHR1YWwKPwoiY2hhcmdlLWFsbERvdWJsZVZlcmlmeUJvdEF2b2lkYW5jZSIZCOf_
_________wESDGRvdWJsZXZlcmlmeQowCgxjaGFyZ2UtYWxsLTEiIAj__________8BEhN0dGRfZGF0YV9leGNsdXNpb25z
```

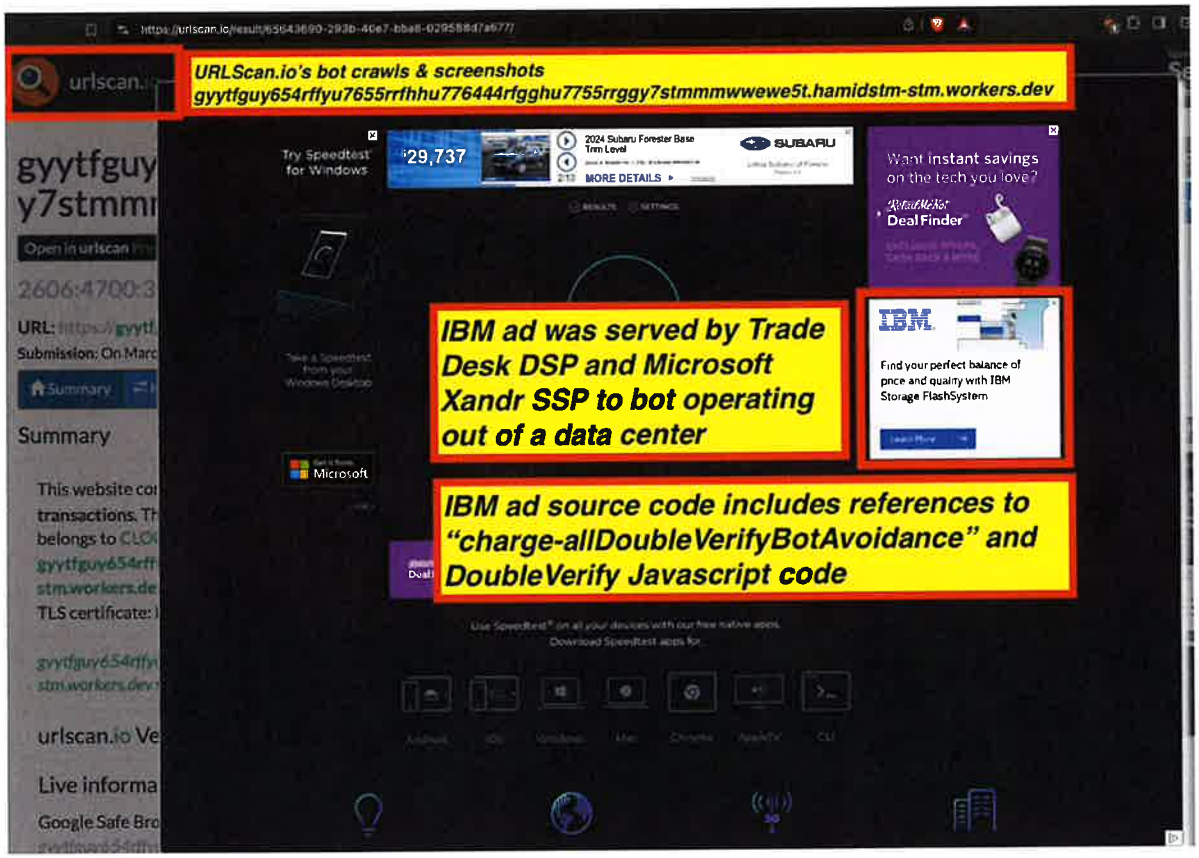
320 1

```
>
!charge-maxDoubleVerifyBrandSafety" · Úô  ÆF+V&ÆWfW&·g·£°¡Ö6·  &vRÖ -ÆÂEDD7W7FöÖ6öçFW·GV -Â! ·¯  Sttdcontextual
?
"charge-allDoubleVerifyBotAvoidance"  çô  ÆF+V&ÆWfW&·g·£·  Æ6·  &vRÖ - ÆÂÖ " · -ÂD·Ý   Û -] WU^ Û \Ù[Û·
```

Source: https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Q2o0S0lXTm9ZWEpuWlMxdFlYaEViM1ZpYkdWV1pYSnBabmxDY21GdVpGTmhabVYwZVNJWkNOdl9fX19fX19fX193RVNER1J2ZFdKc1pYWmxjbWxtZVFvN0NoMWphR0Z5WjJVdFlXeHNWRlJFUTNaVFdEMjl1ZEdWNGRIVmhiQ0lhQ05yX19fX19fX19fX3dFU0RYUjBaR052Ym5SbGVIUjFZV3dLUHdvaVkyaGhjbWRsTFdGc2JFUnZkV0pzWlZabGNtbG1lVUp2ZEVGMmIybGtZVzVqWlNJWkNPZl9fX19fX19fX193RVNER1J2ZFdKc1pYWmxjbWxtZVFvd0NneGphR0Z5WjJVdFlXeHNMVEVpSUFqX19fX19fX19fXzg0QkVoTjBkR1JmWkdGMFlWOWxlR05zZFhOcGIyNXo

As a third example, IBM ads were observed being served to bots operating out of data centers. Many of the IBM ads observed being served to bots in data centers contained Javascript from doubleverify.com and source code from a demand side platform, which included Base64 encoded text.

For example, the IBM ad served was served to a bot that was crawling the website gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev (source: https://urlscan.io/result/65643690-293b-40e7-bba8-029588d7a677/). The URLScan.io bot was operating out of a data center when it was served the IBM ad. The ad was transacted by Trade Desk and Microsoft Xandr SSP.

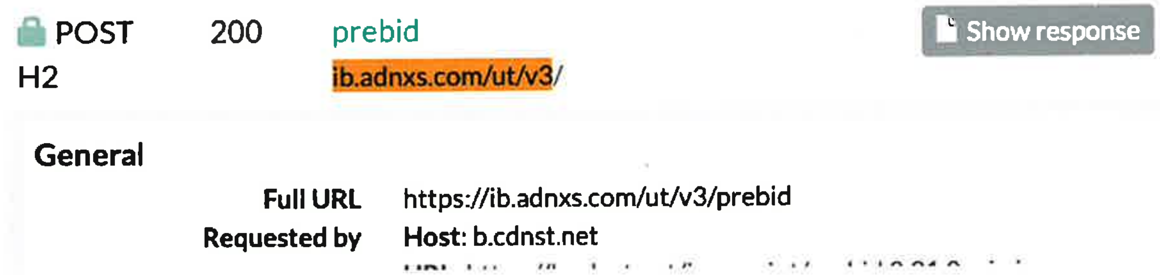


URLScan.io's bot crawls & screenshots gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev

IBM ad was served by Trade Desk DSP and Microsoft Xandr SSP to bot operating out of a data center

IBM ad source code includes references to "charge-allDoubleVerifyBotAvoidance" and DoubleVerify Javascript code

URLScan.io bot screenshot generated when the bot was operating out of a data center and crawling gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev. The bot was served an IBM ad by the Trade Desk and Microsoft Xandr SSP. The source code of the IBM ad includes base64 encoded references to "charge-allDoubleVerifyBotAvoidance"



POST H2 200 prebid ib.adnxs.com/ut/v3/

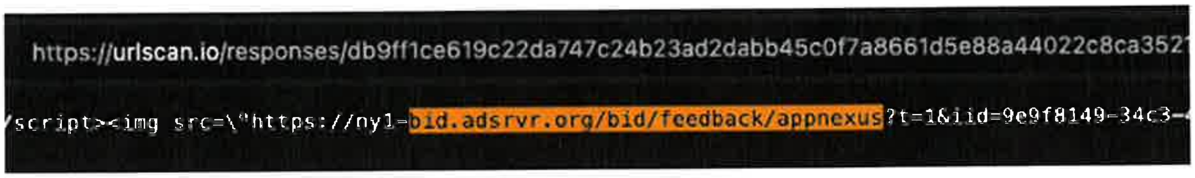
General

Full URL https://ib.adnxs.com/ut/v3/prebid

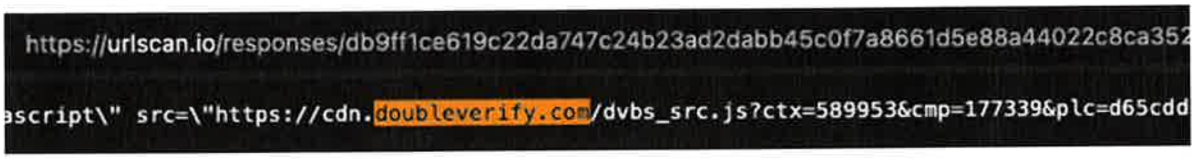
Requested by Host: b.cdnst.net

Screenshot of URLScan.io, showing a POST HTTP request was made to ib.adnxs.com/ut/v3, a Prebid header bidding endpoint operated by Microsoft Xandr (f/k/a AppNexus).

One can inspect the HTTP response from Microsoft Xandr's server to see that the bid response that was transacted by Microsoft Xandr supply side platform (which owns the endpoint ib.adnxs.com/ut/v3/prebid) and by the demand side platform Trade Desk.



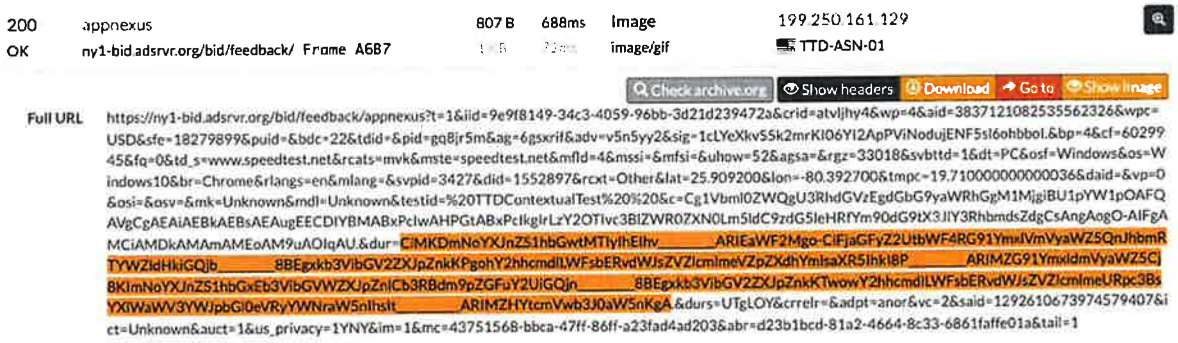
```
https://urlscan.io/responses/db9ff1ce619c22da747c24b23ad2dabb45c0f7a8661d5e88a44022c8ca352

/script><img src=\"https://ny1-bid.adsrvr.org/bid/feedback/appnexus?t=1&iid=9e9f8149-34c3-
```



```
https://urlscan.io/responses/db9ff1ce619c22da747c24b23ad2dabb45c0f7a8661d5e88a44022c8ca352

ascript\" src=\"https://cdn.doubleverify.com/dvbs_src.js?ctx=589953&cmp=177339&plc=d65cdd
```

Screenshots of source code of an HTTP bid response from OpenX's prebid endpoint, when serving a IBM ad to a bot in a data center. Source: https://urlscan.io/responses/db9ff1ce619c22da747c24b23ad2dabb45c0f7a8661d5e88a44022c8ca3521a6/

One can carefully analyze the Trade Desk demand side platform win notification pixel that was triggered when the IBM ad was served to the bot operating out of the data center whilst crawling the website gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev.



```
200   appnexus                                     807 B   688ms   Image        199.250.161.129
OK    ny1-bid.adsrvr.org/bid/feedback/  Frame  A6B7                image/gif    TTD-ASN-01
```

Full URL
```
https://ny1-bid.adsrvr.org/bid/feedback/appnexus?t=1&iid=9e9f8149-34c3-4059-96bb-3d21d239472a&crid=atvljhy4&wp=4&aid=3837121082535562326&wpc=USD&sfe=18279899&puid=&bdc=22&tdid=&pid=gq8jr5m&ag=6gsxrif&adv=v5n5yy2&sig=1cLYeXkvS5k2mrKI06YI2ApPViNodujENF5sl6ohbbol.&bp=4&cf=6029945&fq=0&td_s=www.speedtest.net&rcats=mvk&mste=speedtest.net&mfld=4&mssi=&mfsi=&uhow=52&agsa=&rgz=33018&svbttd=1&dt=PC&osf=Windows&os=Windows10&br=Chrome&rlangs=en&mlang=&svpid=3427&did=1552897&rcxt=Other&lat=25.909200&lon=-80.392700&tmpc=19.710000000000036&daid=&vp=0&osi=&osv=&mk=Unknown&mdl=Unknown&testid=%20TTDContextualTest%20%20&c=Cg1Vbml0ZWQgU3RhdGVzEgdGbG9yaWRhGgM1MjgiBU1pYW1pOAFQAVgCgAEAiAEBkAEBsAEAugEECDIYBMABxPclwAHPGtABxPclkgIrLzY2OTIvc3BlZWR0ZXN0Lm5ldC9zdG5leHRfYm90dG9tX3JlY3RhbmdsZdgCsAngAogO-AIFgAMCiAMDkAMAmAMEoAM9uAOIqAU.&dur=CiMKDmNoYXJnZS1hbGwtMTIylhElhv________ARIEaWF2Mgo-CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjb________8BEgxkb3VibGV2ZXJpZnkKPgohY2hhcmdlLWFsbERvdWJsZVZlcmlmeVZpZXdhYmlsaXR5IhkI8P________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9pZGFuY2UiGQjn________8BEgxkb3VibGV2ZXJpZnkKTwowY2hhcmdlLWFsbERvdWJsZVZlcmlmeURpc3BsYXlWaWV3YWJpbGl0eVRyYWNraW5nIhsIt________ARIMZHYtcmVwb3J0aW5nKgA&durs=UTgLOY&crrelr=&adpt=anor&vc=2&said=1292610673974579407&ict=Unknown&auct=1&us_privacy=1YNY&im=1&mc=43751568-bbca-47ff-86ff-a23fad4ad203&abr=d23b1bcd-81a2-4664-8c33-6861faffe01a&tail=1
```

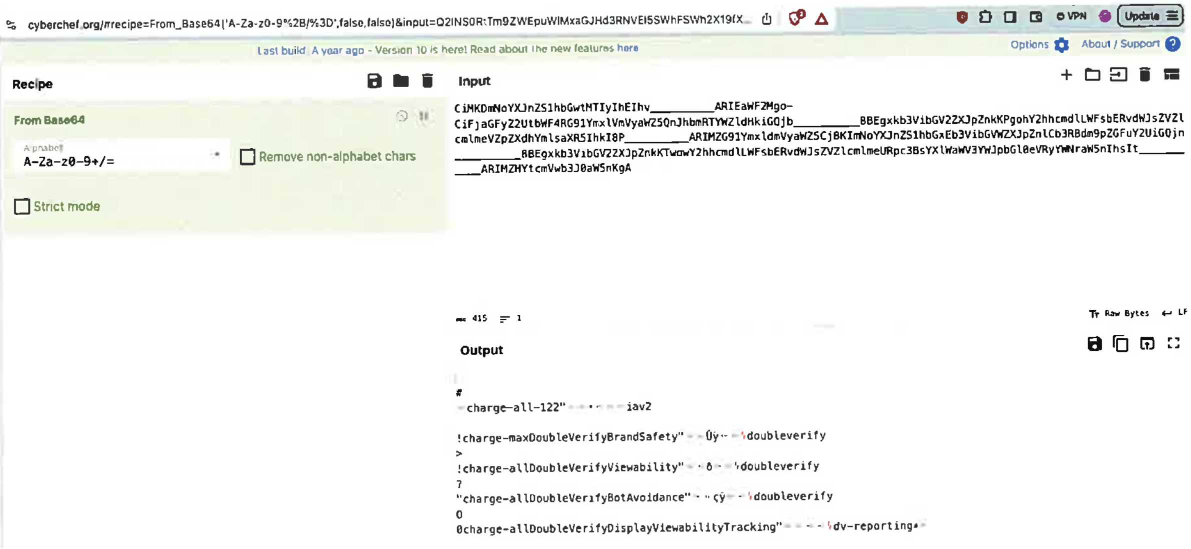
The IBM ad includes a DSP win notification pixel with the "dur=" query string parameter.

The value of the "dur=" query string parameter from the US Navy DSP win notification pixel is a base64 encoded string: "CiMKDmNoYXJnZS1hbGwtMTIylhElhv________ARIEaWF2Mgo-

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjb________8BEgxkb3VibGV2ZXJpZnkKPgohY2hhcmdlLWFsbERvdWJsZVZlcmlmeVZpZXdhYmlsaXR5IhkI8P__________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9pZGFuY2UiGQjn__________8BEgxkb3VibGV2ZXJpZnkKTwowY2hhcmdlLWFsbERvdWJsZVZlcmlmeURpc3BsYXlWaWV3YWJpbGl0eVRyYWNraW5nIhsIt__________ARIMZHYtcmVwb3J0aW5nKgA".

If one copies that specific "dur=" query string parameter and opens the website cyberchef.org (an online web utility or tool provided by the UK signal intelligence agency GCHQ that helps Base64 decode text), one can see the decoded value of this specific "dur=" query string parameter. cyberchef.org shows that the decoded value of the "dur=" query string parameter from the Ikea ad contains references to "charge-allDoubleVerifyBotAvoidance".


cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',false,false)&input=Q2INS0RtTm9ZWEpuWlMxaGJHd3RNVEI5SWhFSWh2X19fX...
VPN
Update
Last build: A year ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
□ Remove non-alphabet chars
□ Strict mode
Input
415
1
Raw Bytes
LF
Output

```
CiMKDmNoYXJnZS1hbGwtMTIyIhEIhv__________ARIEaWF2Mgo-
CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjb__________8BEgxkb3VibGV2ZXJpZnkKPgohY2hhcmdlLWFsbERvdWJsZVZl
cmlmeVZpZXdhYmlsaXR5IhkI8P__________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9pZGFuY2UiGQjn
__________8BEgxkb3VibGV2ZXJpZnkKTwowY2hhcmdlLWFsbERvdWJsZVZlcmlmeURpc3BsYXlWaWV3YWJpbGl0eVRyYWNraW5nIhsIt______
____ARIMZHYtcmVwb3J0aW5nKgA
```

```
#
charge-all-122"       iav2

!charge-maxDoubleVerifyBrandSafety"   Ûy   doubleverify
>
!charge-allDoubleVerifyViewability"   ð   doubleverify
7
"charge-allDoubleVerifyBotAvoidance"   çÿ   doubleverify
0
0charge-allDoubleVerifyDisplayViewabilityTracking"     dv-reporting
```

Source: https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',false,false)&input=Q2INS0RtTm9ZWEpuWlMxaGJHd3RNVEI5SWhFSWh2X19fX19fX19fX0FSSUVhV0YyTWdvLUNpRmphR0Z5WjJVdGJXRjRSRzkxWW14bFZtVnlhV1o1UW5KaGJtUlRZV1psZEhraUdRamJfX19fX19fX19fOEJFZ3hrYjNWaWJHVjJaWEpwWm5rS1Bnb2hZMmhoY21kbExXRnNiRVJ2ZFdKc1pWWmxjbWxtZVZacFpYZGhZbWxzYVhSNUlodkk4UF9fX19fX19fX19BUklNWkc5MWJteGtkbVZ5YVdaNUNqOEtJbU5vWVhKblpTMWhiR3hFYjNWaWJHVldaWEpwWm5sQ2IzUkJkbTlwWkdGdVkyVWlHUWpuX19fX19fX19fXzhCRWd4a2IzVmliR1YyWlhKcFpua0tUd293WTJoaGNtZGxMV0ZzYkVSdlpXSnNaVlpsY21sbWVVUnBjM0JzWVhsV2FXVjNZV0pwYkdsMGVWUnlZV05yYVc1bkloc0l0X19fX19fX19fX0FSSU1aSFl0Y21Wd2IzSjBhVzVuS2dBWVY0pwY

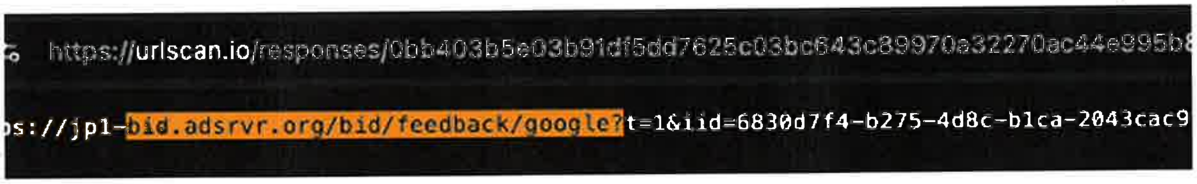
[On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?](https://adalytics.io/blog/prebid-bot-filtration)

kdsMGVWUnlZV05yYVc1bkloc0l0X19fX19fX19fX19BUklNWkhZdGNtVndi M0owYVc1bktnQQ

As a fourth example, Singaporean Government ads were observed being served to bots operating out of data centers. Many of the Singaporean Government ads observed being served to bots in data centers contained source code from a demand side platform, which included Base64 encoded text.

For example, a Singaporean Government ad was served to a bot that was crawling the website ihwal.id. (source: https://urlscan.io/result/50a3059f-ec17-4135-ba2b-563de4bc9b9a/). The URLScan.io bot was operating out of a data center when it was served the Singaporean Government ad. The ad was transacted by Trade Desk and Google AdX.

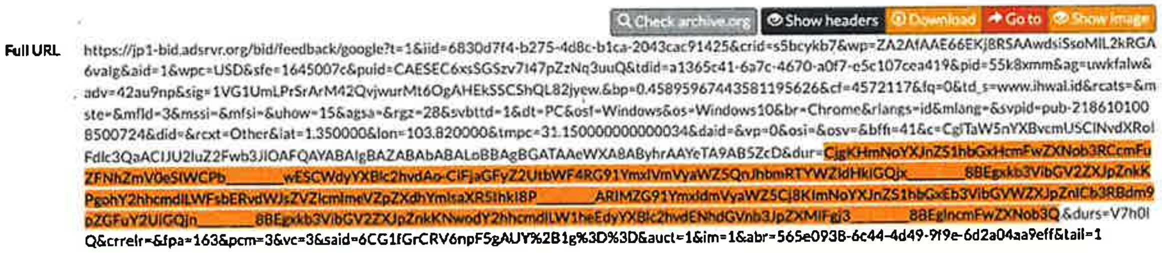
One can inspect the HTTP response from Google's server to see that the bid response was transacted by Google AdX (which owns the endpoint googleads.g.doubleclick.net) and by the demand side platform Trade Desk.



```
https://urlscan.io/responses/0bb403b5e03b91df5dd7625c03bc643c89970a32270ac44e995b8

s://jp1-bid.adsrvr.org/bid/feedback/google?t=1&iid=6830d7f4-b275-4d8c-b1ca-2043cac9
```

Screenshots of source code of an HTTP bid response from Google AdX, when serving a Singaporean Government ad to a bot in a data center. Source: https://urlscan.io/responses/0bb403b5e03b91df5dd7625c03bc643c89970a32270ac44e995b88f84bdea8da/

One can carefully analyze the Trade Desk demand side platform win notification pixel that was triggered when the Singaporean Government ad was served to the bot operating out of the data center whilst crawling the website ihwal.id.



Full URL

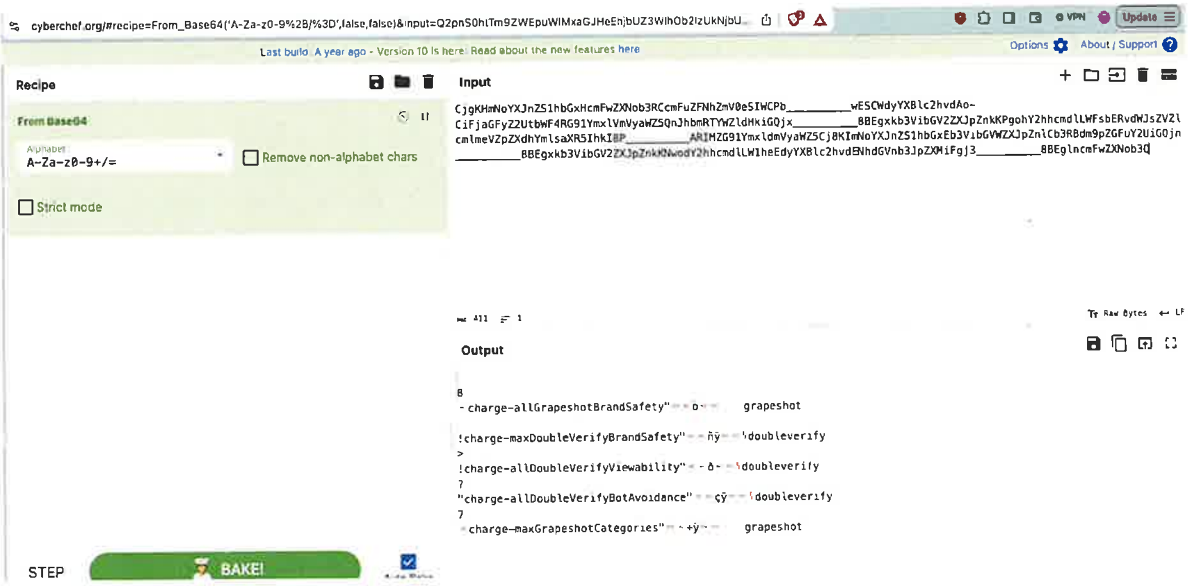
```
https://jp1-bid.adsrvr.org/bid/feedback/google?t=1&iid=6830d7f4-b275-4d8c-b1ca-2043cac91425&crid=s5bcykb7&wp=ZA2AfAAE66EKj8RSAAwdsiSsoMIL2kRGA
6vaig&aid=1&wpc=USD&sfe=1645007c&puid=CAESEC6xsSGSzv7I47pZzNq3uuQ&tdid=a1365c41-6a7c-4670-a0f7-e5c107cea419&pid=55k8xmm&ag=uwkfalw&
adv=42au9np&sig=1VG1UmLPrSrArM42QvjwurMt6OgAHEkSSCShQL82jyew.&bp=0.45895967443581195626&cf=4572117&fq=0&td_s=www.ihwal.id&rcats=&m
ste=&mfld=3&mssi=&mfsi=&uhow=15&agsa=&rgz=28&svbttd=1&dt=PC&osf=Windows&os=Windows10&br=Chrome&rlangs=id&mlang=&svpid=pub-218610100
8500724&did=&rcxt=Other&lat=1.350000&lon=103.820000&tmpc=31.15000000000034&daid=&vp=0&osi=&osv=&bffi=41&c=CglTaW5nYXBvcmUSCINvdXRol
Fdlc3QaACIJU2luZ2Fwb3JlOAFQAYABAIgBAZABAbABALoBBAgBGATAAeWXA8AByhrAAYeTA9AB5ZcD&dur=CjgKHmNoYXJnZS1hbGxHcmFwZXNob3RCcmFu
ZFNhZmV0eSIWCPb________wESCWdyYXBlc2hvdAo-CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjx________8BEgxkb3VibGV2ZXJpZnkK
PgohY2hhcmdlLWFsbERvdWJsZVZlcmlmeVZpZXdhYmlsaXR5IhkI8P________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9
pZGFuY2UiGQjn________8BEgxkb3VibGV2ZXJpZnkKNwodY2hhcmdlLW1heEdyYXBlc2hvdENhdGVnb3JpZXMiFgj3________8BEglncmFwZXNob3Q&durs=V7h0I
Q&crrelr=&fpa=163&pcm=3&vc=3&said=6CG1fGrCRV6npF5gAUY%2B1g%3D%3D&auct=1&im=1&abr=565e093B-6c44-4d49-9f9e-6d2a04aa9eff&tail=1
```

Source: https://urlscan.io/result/50a3059f-ec17-4135-ba2b-563de4bc9b9a/#transactions

The Singaporean Government ad includes a DSP win notification pixel with the "dur=" query string parameter.

The value of the "dur=" query string parameter from the US Navy DSP win notification pixel is a base64 encoded string: "CjgKHmNoYXJnZS1hbGxHcmFwZXNob3RCcmFuZFNhZmV0eSIWCPb__________wESCWdyYXBlc2hvdAo-CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjx__________8BEgxkb3VibGV2ZXJpZnkKPgohY2hhcmdlLWFsbERvdWJsZVZlcmlmeVZpZXdhYmlsaXR5IhkI8P__________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9pZGFuY2UiGQjn__________8BEgxkb3VibGV2ZXJpZnkKNwodY2hhcmdlLW1heEdyYXBlc2hvdENhdGVnb3JpZXMiFgj3__________8BEglncmFwZXNob3Q".

If one copies that specific "dur=" query string parameter and opens the website cyberchef.org (an online web utility or tool that helps Base64 decode text), one can see the decoded value of this specific "dur=" query string parameter. cyberchef.org shows that the decoded value of the "dur=" query string parameter from the Ikea ad contains references to "charge-allDoubleVerifyBotAvoidance".


cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',false,false)&input=Q2pnS0hiTm9ZWEpuWlMxaGJHeEhjbUZ3WlhOb2lzUkNjbU...
VPN
Update
Last build: A year ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
☐ Remove non-alphabet chars
☐ Strict mode
Input
411
1
Tr Raw Bytes
LF
Output
STEP
BAKE!
☑

CjgKHmNoYXJnZS1hbGxHcmFwZXNob3RCcmFuZFNhZmV0eSIWCPb__________wESCWdyYXBlc2hvdAo-
CiFjaGFyZ2UtbWF4RG91YmxlVmVyaWZ5QnJhbmRTYWZldHkiGQjx__________8BEgxkb3VibGV2ZXJpZnkKPgohY2hhcmdlLWFsbERvdWJsZVZlcmlmeVZpZXdhYmlsaXR5IhkI8P__________ARIMZG91YmxldmVyaWZ5Cj8KImNoYXJnZS1hbGxEb3VibGVWZXJpZnlCb3RBdm9pZGFuY2UiG0jn__________8BEgxkb3VibGV2ZXJpZnkKNwodY2hhcmdlLW1heEdyYXBlc2hvdENhdGVnb3JpZXMiFgj3__________8BEglncmFwZXNob3Q

```
8
- charge-allGrapeshotBrandSafety"  ö    grapeshot

!charge-maxDoubleVerifyBrandSafety"  ñÿ  doubleverify
>
!charge-allDoubleVerifyViewability" - ð-  doubleverify
?
"charge-allDoubleVerifyBotAvoidance"  çÿ  doubleverify
7
 charge-maxGrapeshotCategories" +ÿ-    grapeshot
```

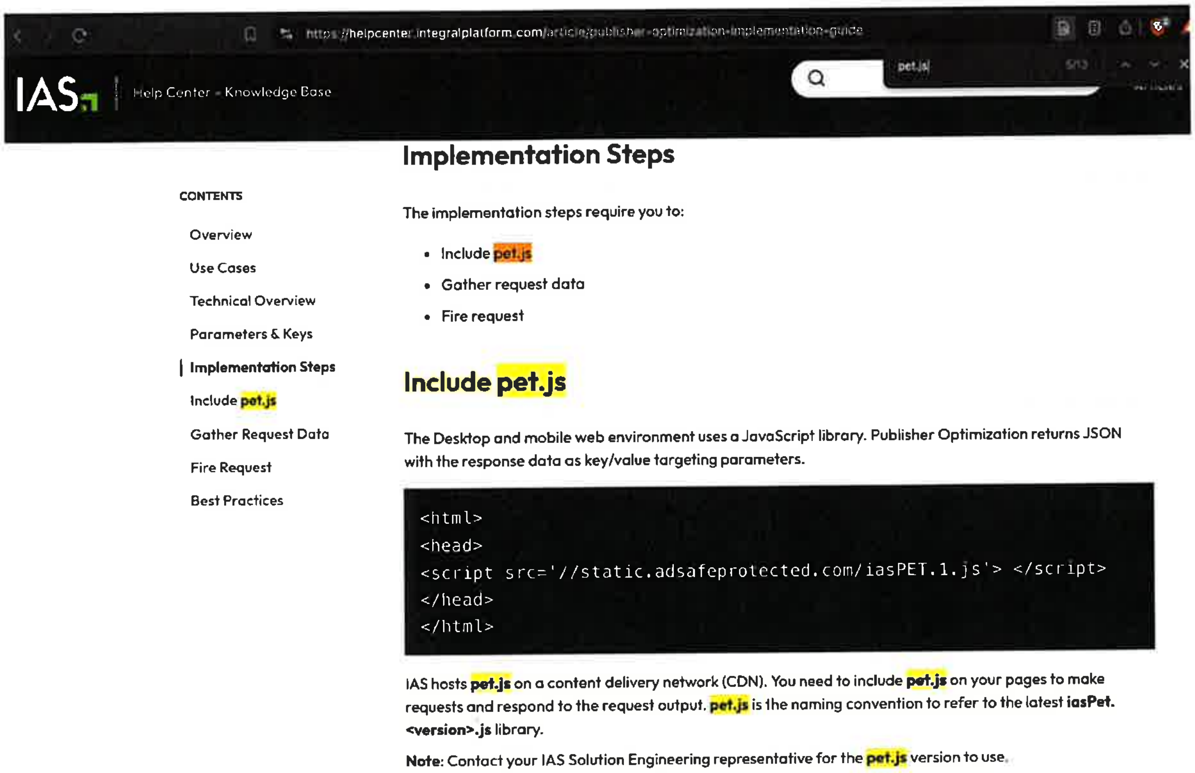
Source: https://cyberchef.org/#recipe=From_Base64('A-Za-z0-9%2B/%3D',false,false)&input=Q2pnS0htTm9ZWEpuWlMxaGJHeEhjbUZ3WlhOb2IzUkNjbUZ1WkZOaFptVjBlU0lXQ1BiX19fX19fX19fX3dFU0NXZHlZWEJsYzJodmRBby1DaUZqYUdGeVoyVXRiV0Y0Ukc5MVlteGxWbVZ5YVdaNVFuSmhibVJUWVdabGRIa2lHUWp4X19fX19fX19fXzhCRWd4a2IzVmliR1YyWlhKcFpua0tQZ29oWTJoaGNtZGxMV0ZzYkVSdmRXSnNaVlpsY21sbWVWWnBaWGRoWW1sc2FYUjVJaGtJOFBfX19fX19fX19fQVJJTVpHOTFZbXhsZG1WeWFXWjVDajhLSW1Ob1lYSm5aUzFoYkd4RWIzVmliR1ZXWlhKcFpubENiM1JCZG05cFpHRnVZMlVpRzBqbl9fX19fX19fX184QkVneGtiM1ZpYkdWMlpYSnBabmtLTndvZFkyaGhjbWRsTFcxaGVFZHlZWEJsYzJodmRFTmhkR1ZuYjNKcFpYTWlGZ2ozX19fX19fX19fXzhCRWdsbmNtRndaWE5vYjNR

Research Results

Research Results: IAS's publisher services pixel appears to label bots as valid human traffic in certain occasions

IAS's public "Publisher Optimization Implementation Guide" explains that the "The desktop and mobile web environment uses a JavaScript library. Publisher Optimization returns JSON with the response data as key/valu

Jo e targeting parameters." This is loaded via a specific Javascript file called: "static.adsafeprotected.com/iasPET.1.js".


https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide
IAS
Help Center - Knowledge Base
pet.js
5/13

Implementation Steps

CONTENTS

- Overview
- Use Cases
- Technical Overview
- Parameters & Keys
- Implementation Steps
- Include pet.js
- Gather Request Data
- Fire Request
- Best Practices

The implementation steps require you to:

- Include pet.js
- Gather request data
- Fire request

Include pet.js

The Desktop and mobile web environment uses a JavaScript library. Publisher Optimization returns JSON with the response data as key/value targeting parameters.

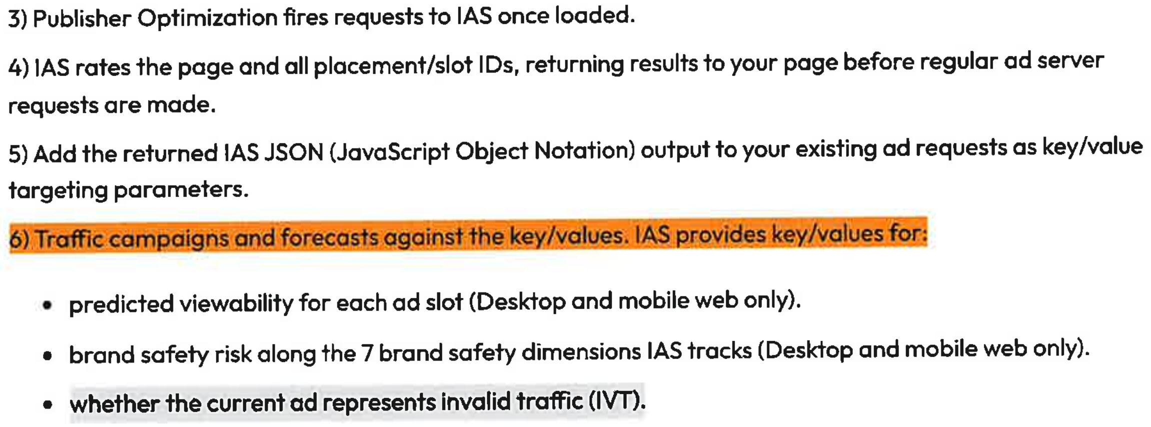
```
<html>
<head>
<script src='//static.adsafeprotected.com/iasPET.1.js'> </script>
</head>
</html>
```

IAS hosts **pet.js** on a content delivery network (CDN). You need to include **pet.js** on your pages to make requests and respond to the request output. **pet.js** is the naming convention to refer to the latest **iasPet.<version>.js** library.

Note: Contact your IAS Solution Engineering representative for the **pet.js** version to use.

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link: https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

The IAS Publisher Optimization tool "provides key/values for: [...] whether the current ad represents invalid traffic (IVT)."



3) Publisher Optimization fires requests to IAS once loaded.

4) IAS rates the page and all placement/slot IDs, returning results to your page before regular ad server requests are made.

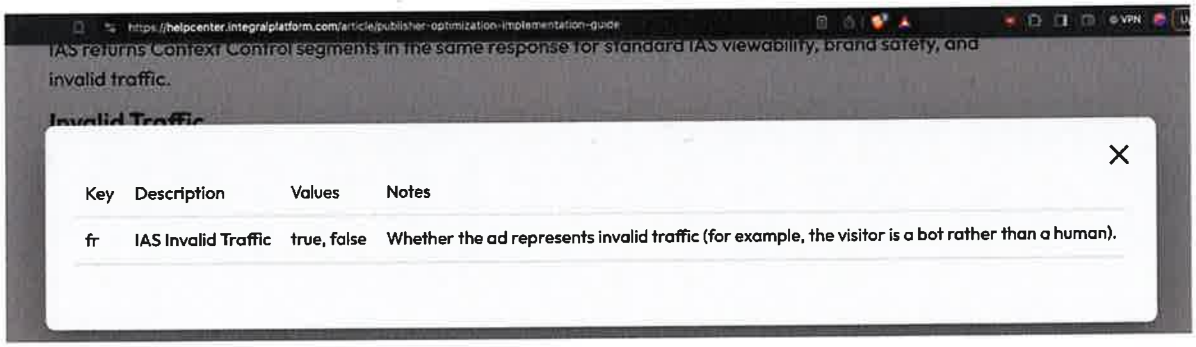
5) Add the returned IAS JSON (JavaScript Object Notation) output to your existing ad requests as key/value targeting parameters.

6) Traffic campaigns and forecasts against the key/values. IAS provides key/values for:

- predicted viewability for each ad slot (Desktop and mobile web only).
- brand safety risk along the 7 brand safety dimensions IAS tracks (Desktop and mobile web only).
- whether the current ad represents invalid traffic (IVT).

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link: https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

IAS's "publisher optimization implementation guide" reveals that the vendor uses the "fr" key to indicate "IAS Invalid Traffic". Possible values for the "fr" key are "fr=true" or "fr=false. The guide explains that this indicates "Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human)."



https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide
VPN

IAS returns Context Control segments in the same response for standard IAS viewability, brand safety, and invalid traffic.

Invalid Traffic

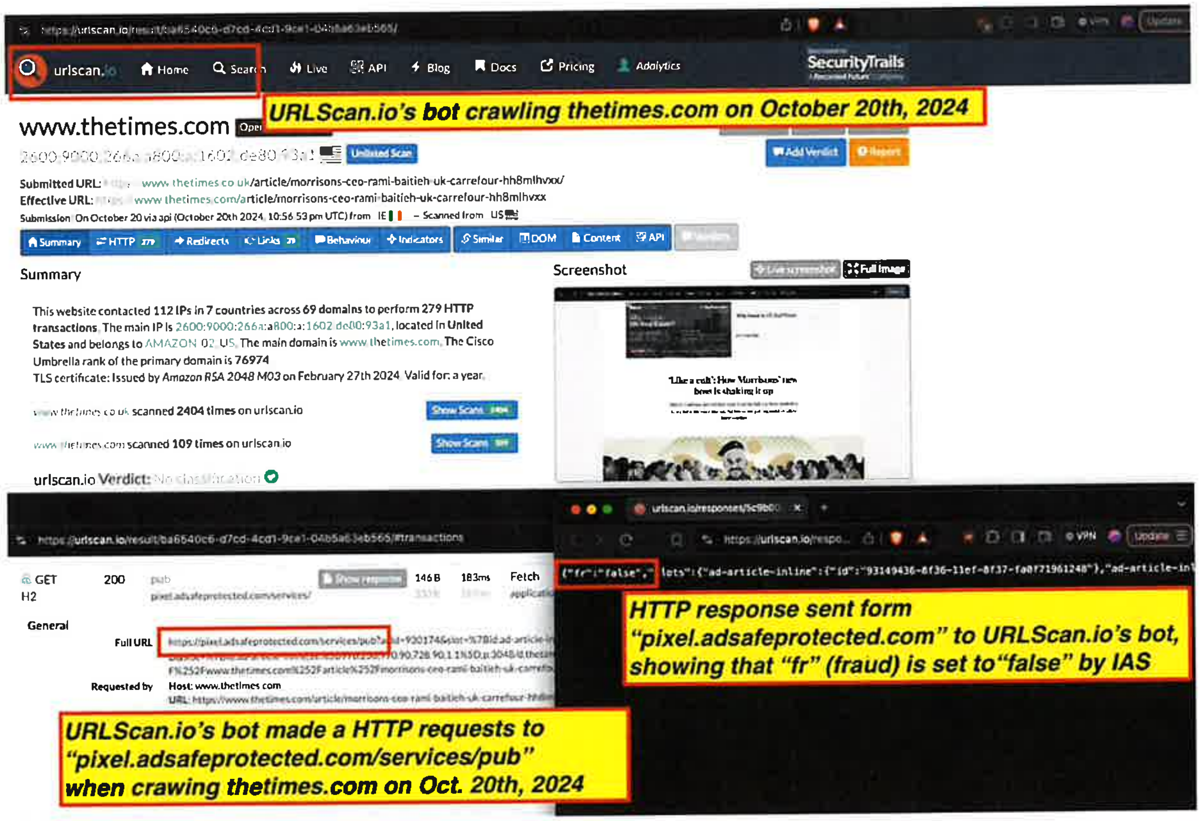
Key	Description	Values	Notes
fr	IAS Invalid Traffic	true, false	Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human).

Screenshot of Integral Ad Science (IAS)'s public "Publisher Optimization Implementation Guide" - Original Link: https://helpcenter.integralplatform.com/article/publisher-optimization-implementation-guide; Archived: https://perma.cc/G6EZ-76VR;

Given a sample dataset of 100% confirmed bot traffic as a ground truth baseline, one can analyze within thesample how often IAS' publisher optimization tool returns a value of "fr=true" (bot) or "fr=false" (not bot).

For example, for a set of bot crawls, one can see whether IAS's "pixel.adsafeprotected.com" endpoint returned a value of "fr=true" or "fr=false".

In the screenshot below, one can see an instance where URLScan.io's bot crawled thetimes.com on October 20th, 2024. One can see that, when the bot was crawling thetimes.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false".



URLScan.io's bot crawling thetimes.com on October 20th, 2024

www.thetimes.com

Submitted URL: www.thetimes.co.uk/article/morrisons-ceo-rami-baitieh-uk-carrefour-hh8mlhvxx/
Effective URL: www.thetimes.com/article/morrisons-ceo-rami-baitieh-uk-carrefour-hh8mlhvxx
Submission: On October 20 via api (October 20th 2024, 10:56:53 pm UTC) from IE — Scanned from US

Summary

This website contacted 112 IPs in 7 countries across 69 domains to perform 279 HTTP transactions. The main IP is 2600:9000:266a:a800:a:1602:de00:93a1, located in United States and belongs to AMAZON-02, US. The main domain is www.thetimes.com. The Cisco Umbrella rank of the primary domain is 76974.
TLS certificate: Issued by Amazon RSA 2048 M03 on February 27th 2024. Valid for: a year.

www.thetimes.co.uk scanned 2404 times on urlscan.io

www.thetimes.com scanned 109 times on urlscan.io

urlscan.io Verdict: No classification

GET H2 200 pub pixel.adsafeprotected.com/services/ 146 B 183ms Fetch

General

Full URL: https://pixel.adsafeprotected.com/services/pub?...

Requested by: Host: www.thetimes.com

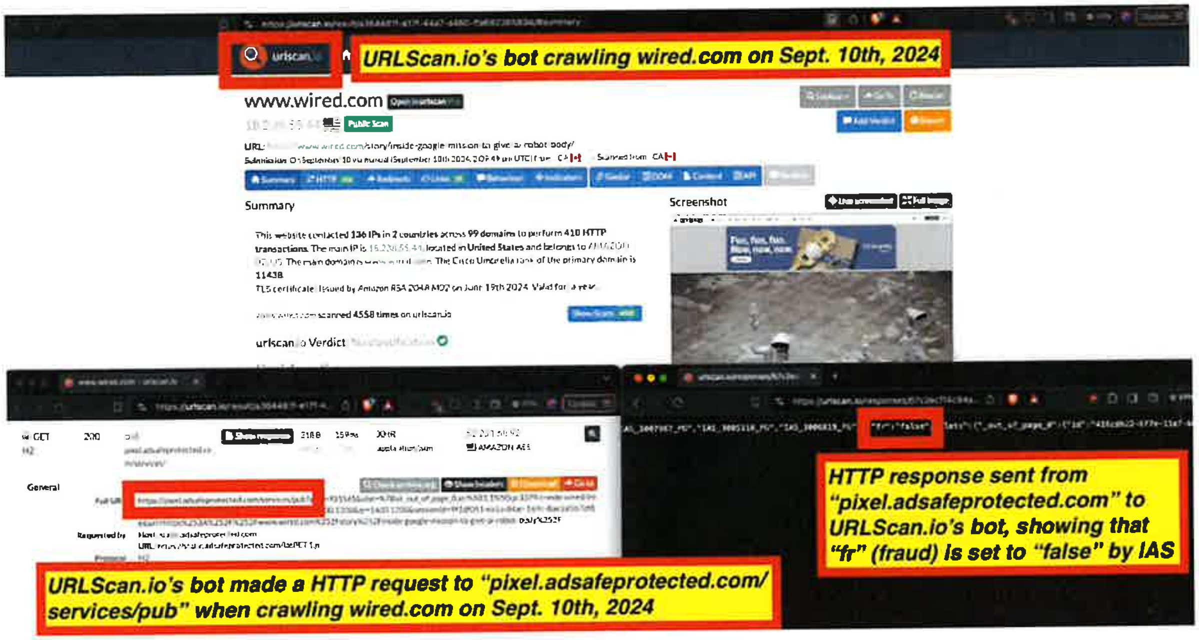
{"fr":"false","slots":{"ad-article-inline":{"id":"93149436-8f36-11ef-8f37-fa0f71961248"},"ad-article-in

HTTP response sent form "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to"false" by IAS

URLScan.io's bot made a HTTP requests to "pixel.adsafeprotected.com/services/pub" when crawing thetimes.com on Oct. 20th, 2024

Composite screenshot of URLScan.io's bot crawling thetimes.com on October 20th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false".

As a second example, in the screenshot below, one can see an instance where URLScan.io's bot crawled wired.com on September 10th, 2024. One can see that, when the bot was crawling wired.com, IAS's server endpoint “pixel.adsafeprotected.com/services/pub” was invoked. That HTTP endpoint returned a JSON response, with the “fr” key value set to “false”, as in “fr=false”. This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic.



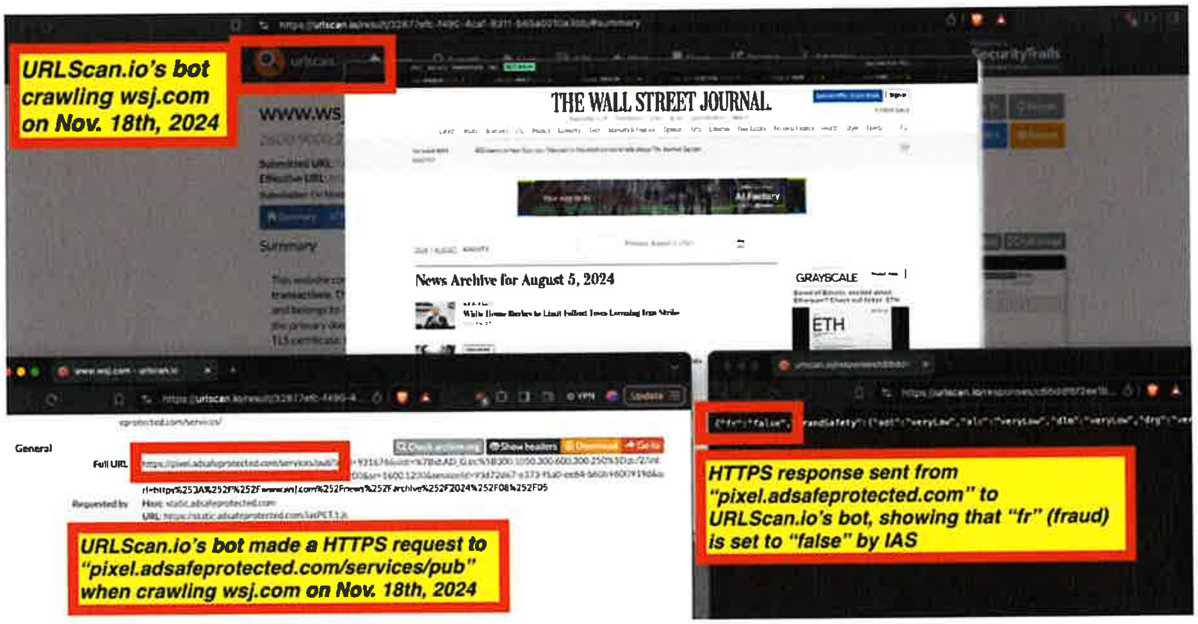
URLScan.io’s bot crawling wired.com on Sept. 10th, 2024

HTTP response sent from “pixel.adsafeprotected.com” to URLScan.io’s bot, showing that “fr” (fraud) is set to “false” by IAS

URLScan.io’s bot made a HTTP request to “pixel.adsafeprotected.com/services/pub” when crawling wired.com on Sept. 10th, 2024

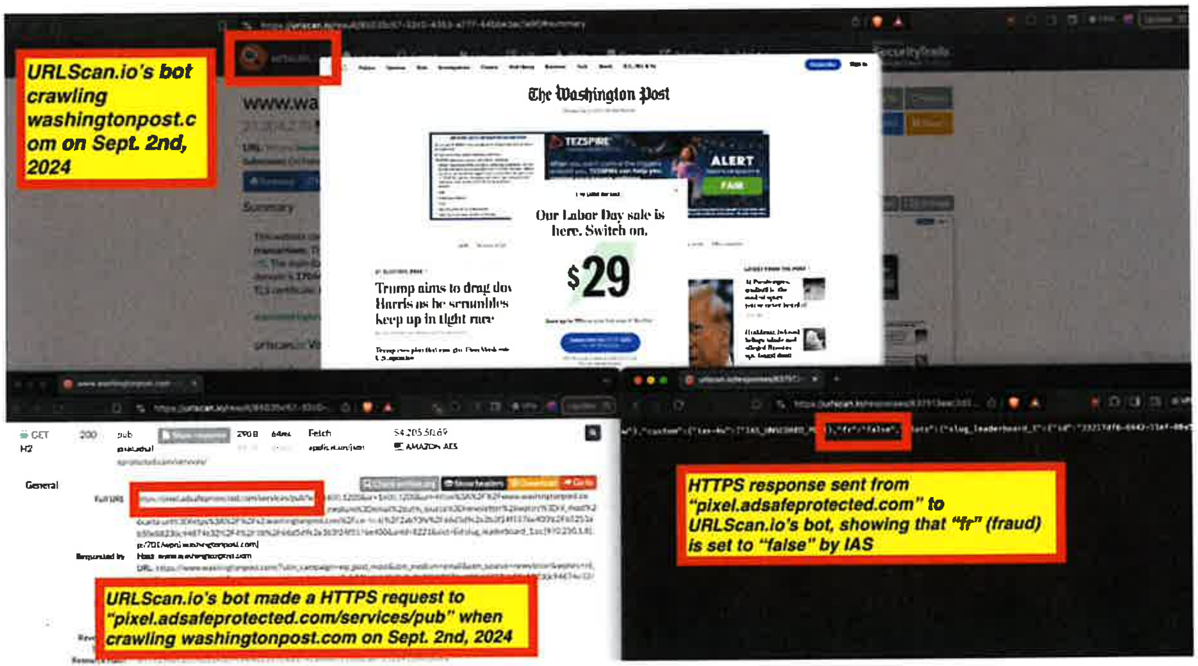
Composite screenshot of URLScan.io’s bot crawling wired.com on September 10th, 2024. The screenshot shows HTTPS requests to “pixel.adsafeprotected.com”, which elicited an HTTPS response with “fr”: “false”.

As a third example, in the screenshot below, one can see an instance where URLScan.io’s bot crawled wsj.com on November 18th, 2024. One can see that, when the bot was crawling wsj.com, IAS’s server endpoint “pixel.adsafeprotected.com/services/pub” was invoked. That HTTP endpoint returned a JSON response, with the “fr” key value set to “false”, as in “fr=false”. This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic.


URLScan.io's bot crawling wsj.com on Nov. 18th, 2024
THE WALL STREET JOURNAL.
News Archive for August 5, 2024
URLScan.io's bot made a HTTPS request to "pixel.adsafeprotected.com/services/pub" when crawling wsj.com on Nov. 18th, 2024
HTTPS response sent from "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to "false" by IAS

Composite screenshot of URLScan.io's bot crawling wsj.com on November 18th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false".

As a fourth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled washingtonpost.com on September 2nd, 2024. One can see that, when the bot was crawling washingtonpost.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false". This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic.



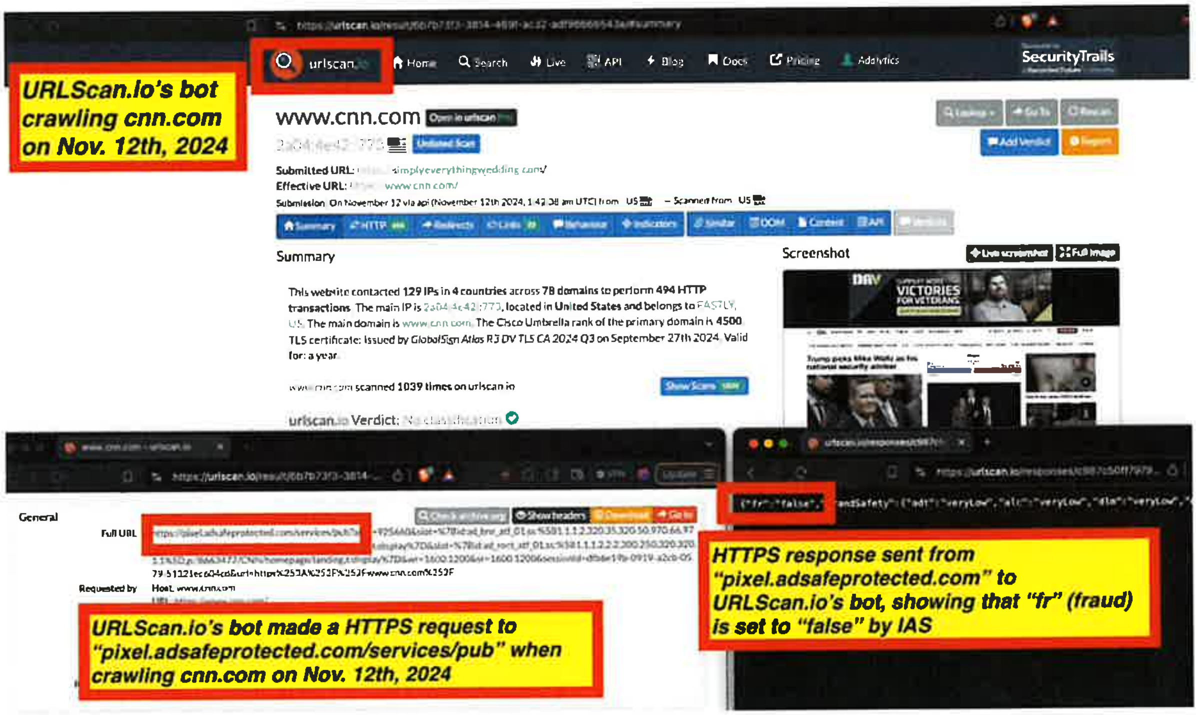
URLScan.io's bot crawling washingtonpost.com on Sept. 2nd, 2024

HTTPS response sent from "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to "false" by IAS

URLScan.io's bot made a HTTPS request to "pixel.adsafeprotected.com/services/pub" when crawling washingtonpost.com on Sept. 2nd, 2024

Composite screenshot of URLScan.io's bot crawling washingtonpost.com on Sept. 2nd, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false".

As a fifth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled cnn.com on November 12th, 2024. One can see that, when the bot was crawling cnn.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false". This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic.



URLScan.io's bot crawling cnn.com on Nov. 12th, 2024

www.cnn.com

Submitted URL: https://simplyeverythingwedding.com/

Effective URL: https://www.cnn.com/

Submission: On November 12 via api (November 12th 2024, 1:42:38 am UTC) from US — Scanned from US

Summary

This website contacted 129 IPs in 4 countries across 78 domains to perform 494 HTTP transactions. The main IP is 2a04:4e42:773, located in United States and belongs to FASTLY, US. The main domain is www.cnn.com. The Cisco Umbrella rank of the primary domain is 4500. TLS certificate: Issued by GlobalSign Atlas R3 DV TLS CA 2024 Q3 on September 27th 2024. Valid for: a year.

www.cnn.com scanned 1039 times on urlscan.io

urlscan.io Verdict: No classification

Host: www.cnn.com

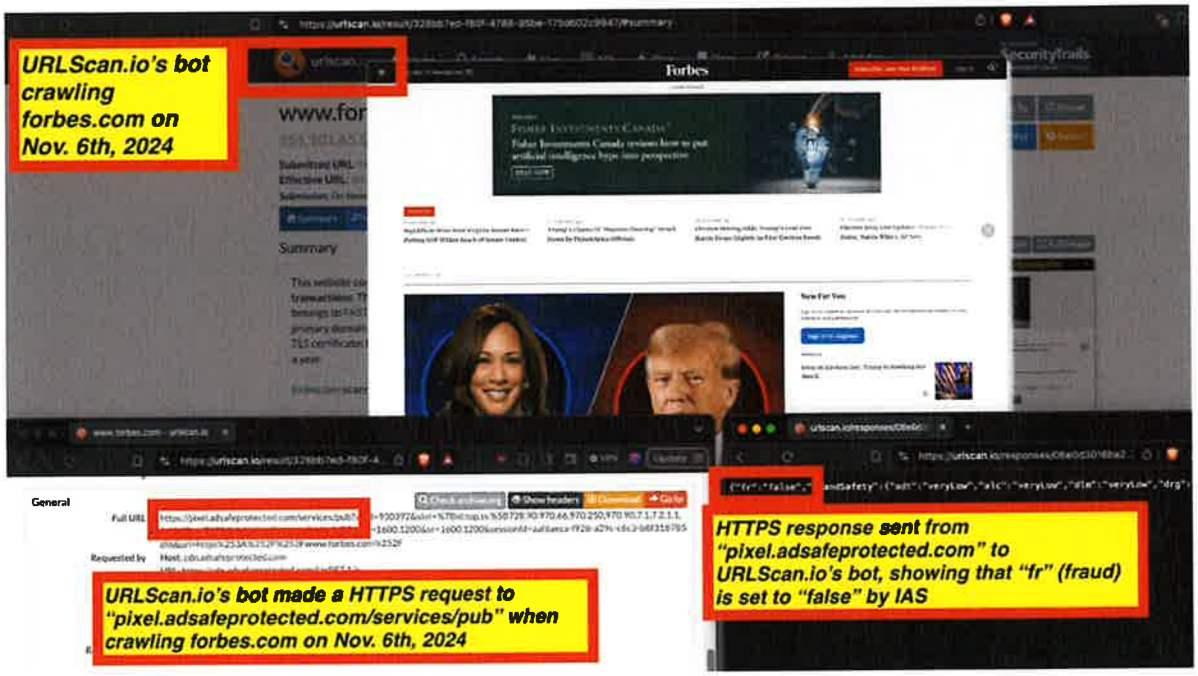
{"fr":"false", ... andSafety":{"adt":"veryLow","alc":"veryLow","dlm":"veryLow",

URLScan.io's bot made a HTTPS request to "pixel.adsafeprotected.com/services/pub" when crawling cnn.com on Nov. 12th, 2024

HTTPS response sent from "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to "false" by IAS

Composite screenshot of URLScan.io's bot crawling cnn.com on Nov 12th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false".

As a sixth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled forbes.com on November 6th, 2024. One can see that, when the bot was crawling forbes.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false". This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic. Forbes also appears to have installed the DoubleVerify publisher optimization tool on its web pages.



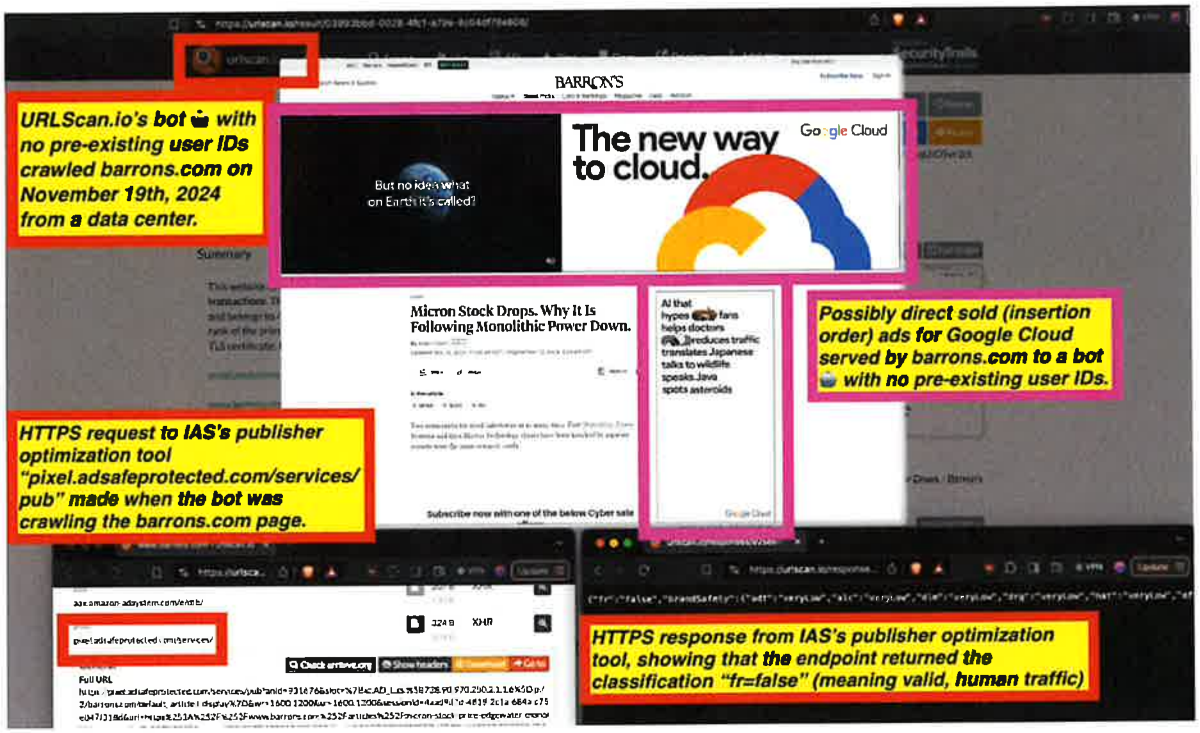
URLScan.io's bot crawling forbes.com on Nov. 6th, 2024

URLScan.io's bot made a HTTPS request to "pixel.adsafeprotected.com/services/pub" when crawling forbes.com on Nov. 6th, 2024

HTTPS response sent from "pixel.adsafeprotected.com" to URLScan.io's bot, showing that "fr" (fraud) is set to "false" by IAS

Composite screenshot of URLScan.io's bot crawling forbes.com on November 6th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false". Forbes also appears to use DoubleVerify's publisher optimization tools on its pages.

As a seventh example, in the screenshot below, one can see an instance where URLScan.io's bot crawled barrons.com on November 19th, 2024. One can see that, when the bot was crawling barrons.com, IAS's server endpoint "pixel.adsafeprotected.com/services/pub" was invoked. That HTTP endpoint returned a JSON response, with the "fr" key value set to "false", as in "fr=false". This suggests that according to IAS's adjudication, the URLScan.io bot does **not** constitute invalid traffic, and is therefore being classified as valid, human traffic.


urlscan
BARRON'S
But no idea what on Earth it's called?
The new way to cloud.
Google Cloud
Micron Stock Drops. Why It Is Following Monolithic Power Down.
Summary
Subscribe now with one of the below Cyber sale
pixel.adsafeprotected.com/services/
Full URL
XHR
Check archive.org
Show headers

URLScan.io's bot 🤖 with no pre-existing user IDs crawled barrons.com on November 19th, 2024 from a data center.

Possibly direct sold (insertion order) ads for Google Cloud served by barrons.com to a bot 🤖 with no pre-existing user IDs.

HTTPS request to IAS's publisher optimization tool "pixel.adsafeprotected.com/services/pub" made when the bot was crawling the barrons.com page.

HTTPS response from IAS's publisher optimization tool, showing that the endpoint returned the classification "fr=false" (meaning valid, human traffic)

Composite screenshot of URLScan.io's bot crawling forbes.com on November 19th, 2024. The screenshot shows HTTPS requests to "pixel.adsafeprotected.com", which elicited an HTTPS response with "fr": "false", suggesting that IAS classified the given request as valid, human traffic. It appears that barrons.com served two potentially direct sold (insertion order) ads for Google Cloud to the bot. Source: https://urlscan.io/result/03993bbd-0028-4fc1-a79e-8c04df78e808/

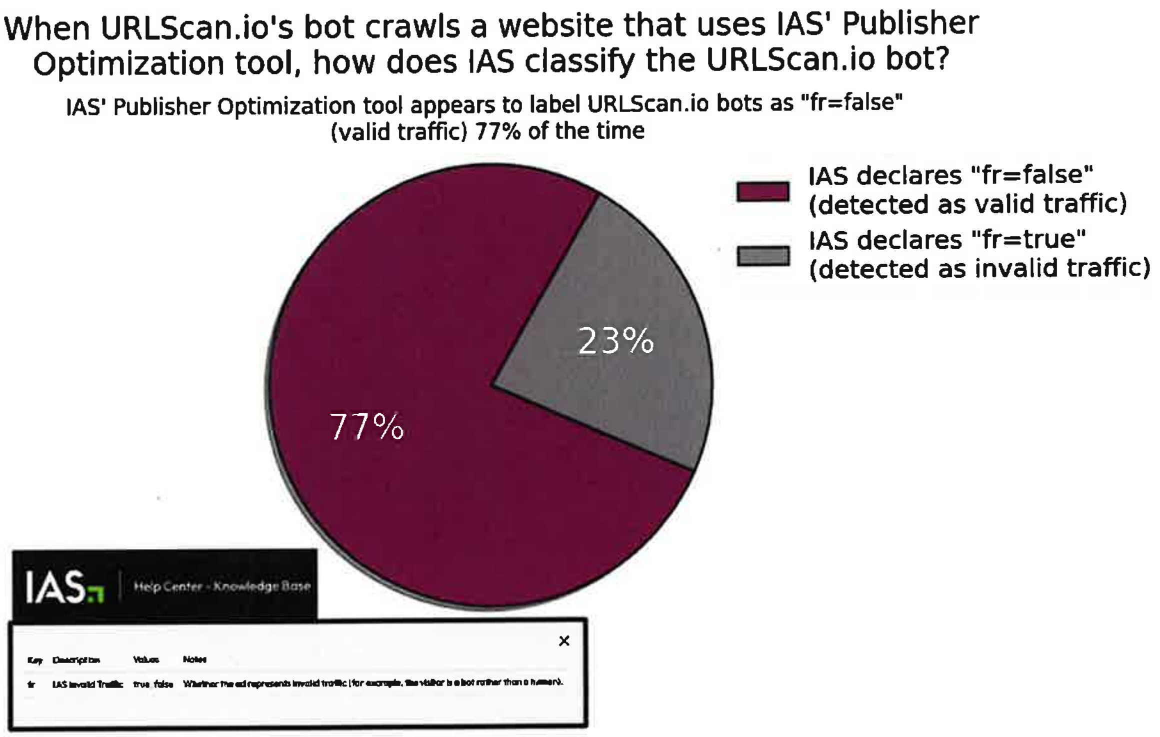
As explained earlier, Urlscan.io is a web-based security tool and public sandbox that analyzes websites by automating the process of visiting URLs with a bot to capture detailed metadata, including HTTP requests, DNS lookups, and visual snapshots, which can be used for threat analysis and research. Urlscan.io automates checking websites with a headless browser bot.

Based on a sample of URLScan.io crawls from 2019 to 2024 (5+ years) across over 1,200 distinct websites in North America, Europe, Japan, Singapore, Australia, and other countries, it is possible to see how often IAS' Publisher Optimization tool labeled URLScan.io's bot as "fr=true" (meaning, invalid traffic or a bot), versus "fr=false" (meaning, valid traffic or a human).

This dataset was compiled from instances where the bot crawled many different websites, including wsj.com, nfl.com, weather.com, cnn.com, forbes.com, americanbanker.com, tripadvisor.com, genius.com, reuters.com, bloomberg.com, washingtonpost.com, businessinsider.com, usatoday.com, wired.com, newyorker.com, vogue.com, vanityfair.com, lefigaro.fr, and others.

In some cases, IAS's Publisher Optimization tool correctly identified URLScan.io's bot as a bot, and labeled it as "fr=true" (meaning it's a bot). In many cases however, URLScan.io's bot crawling a page was labeled as "fr=false".

Across the sample of URLScan.io crawls from 2019-2024, IAS's Publisher Optimization tool labeled the URLScan.io bot as "fr=false" (valid traffic or human) 77% of the time.



When URLScan.io's bot crawls a website that uses IAS' Publisher Optimization tool, how does IAS classify the URLScan.io bot?

IAS' Publisher Optimization tool appears to label URLScan.io bots as "fr=false" (valid traffic) 77% of the time

Key	Description	Values	Notes
fr	IAS Invalid Traffic	true, false	Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human).

One point that merits mentioning is that in some cases, it appears that IAS' publisher optimization tool labeled the same bot and page view session as both valid, human traffic ("fr=false") and simultaneously as invalid, bot traffic ("fr=true").

For example, on March 17th, 2022, URLScan.io's bot crawled the Swiss website 20minuti.ch. The IAS Publisher Optimization endpoint was invoked fifty seven (57x) times whilst the URLScan.io bot was crawling this page on March 17th. Forty (40x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst seventeen (17x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). It is not immediately apparent from IAS' public documentation how situations where a bot is labeled as both valid, human traffic and invalid bot traffic are dispositioned. The URLScan.io crawl record from March 17th, 2022 on 20minuti.ch can be found here: https://urlscan.io/result/be50408e-393b-451d-b571-2b85875c2c5c.

As a second example, on May 21st, 2024, URLScan.io's bot crawled reuters.com. The IAS Publisher Optimization endpoint was invoked seventeen (17x) times whilst the URLScan.io bot was crawling this Reuters page on May 21st, 2024. Nine (9x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst eight (8x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). It is not immediately apparent from IAS' public documentation how situations where a bot is labeled as both valid, human traffic and invalid bot traffic are resolved. The URLScan.io crawl record from May 21st, 2024 on reuters.com can be found here: https://urlscan.io/result/58d84a13-e69e-402e-848e-e01e807c4849 .

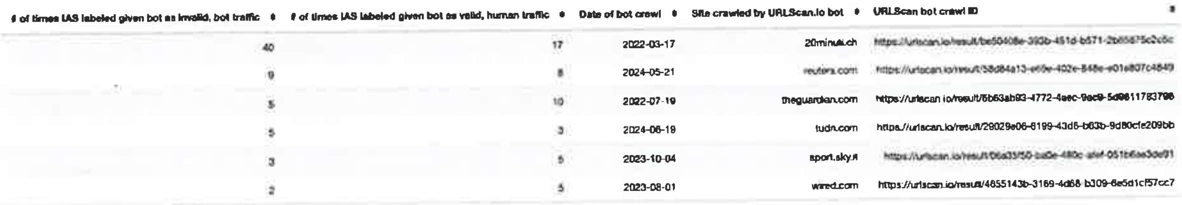
As a third example, on July 19th, 2022, URLScan.io's bot crawled theguardian.com. The IAS Publisher Optimization endpoint was invoked fifteen (15x) times whilst the URLScan.io bot was crawling this The Guardian page on July 19th, 2022. Five (5x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst ten (10x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). The URLScan.io crawl record from July 19th, 2022 on theguardian.com can be found here: https://urlscan.io/result/5b63ab93-4772-4aec-9ac9-5d9611783796.

As a fourth example, on June 19th, 2024, URLScan.io's bot crawled the Mexican-American Spanish language sports website tudn.com (owned by TelevisaUnivision). The IAS Publisher Optimization endpoint was invoked eight (8x) times whilst the URLScan.io bot was crawling this TUDN page on June 19th, 2024. Five (5x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst three (3x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). he URLScan.io crawl record from June 19th, 2024 on tudn.com can be found here: https://urlscan.io/result/29029e06-6199-43d6-b63b-9d80cfe209bb.

As a fifth example, on October 4th, 2023, URLScan.io's bot crawled the Italian sports page sport.sky.it. The IAS Publisher Optimization endpoint was invoked eight (8x) times whilst the URLScan.io bot was crawling this sport.sky.it page on October 4th, 2023. Three (3x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst five (5x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). The URLScan.io crawl record from October 4th, 2023 on sport.sky.it can be found here: https://urlscan.io/result/06a35f50-ba0e-480c-afef-051b6ae3de91.

As a sixth example, on August 1st, 2023, URLScan.io's bot crawled wired.com (owned by Conde Nast). The IAS Publisher Optimization endpoint was invoked seven (7x) times whilst the URLScan.io bot was crawling this wired.com page on August 1st, 2023. Two (2x) of the HTTPS responses from the "pixel.adsafeprotected/services/pub" endpoint indicated the URLScan.io bot was classified as invalid, bot traffic ("fr=true"), whilst five (5x) of the HTTPS responses from the IAS endpoint indicated that the URLScan.io bot was classified as valid, human traffic ("fr=false"). The URLScan.io crawl record from August 1st, 2023 on wired.com can be found here: https://urlscan.io/result/4655143b-3169-4d68-b309-6e5d1cf57cc7.

Below is a summary table of the above examples..



# of times IAS labeled given bot as invalid, bot traffic	# of times IAS labeled given bot as valid, human traffic	Date of bot crawl	Site crawled by URLScan.io bot	URLScan bot crawl ID
40	17	2022-03-17	20minuti.ch	https://urlscan.io/result/be50408e-393b-451d-b571-2b85875c2c5c
9	8	2024-05-21	reuters.com	https://urlscan.io/result/58d84a13-e69e-402e-848e-e01e807c4849
5	10	2022-07-19	theguardian.com	https://urlscan.io/result/5b63ab93-4772-4aec-9ac9-5d9811783798
5	3	2024-06-19	tudn.com	https://urlscan.io/result/29029e06-8199-43d6-b63b-9d80cfe209bb
3	5	2023-10-04	sport.sky.it	https://urlscan.io/result/06a33f50-ba0e-480c-afef-051b6ae3de91
2	5	2023-08-01	wired.com	https://urlscan.io/result/4655143b-3169-4d88-b309-6e5d1cf57cc7

Table illustrating examples where IAS' publisher optimization tool ('pixel.adsafeprotected.com/services/pub') returned multiple distinct "fr" classifications for the same URLScan.io bot

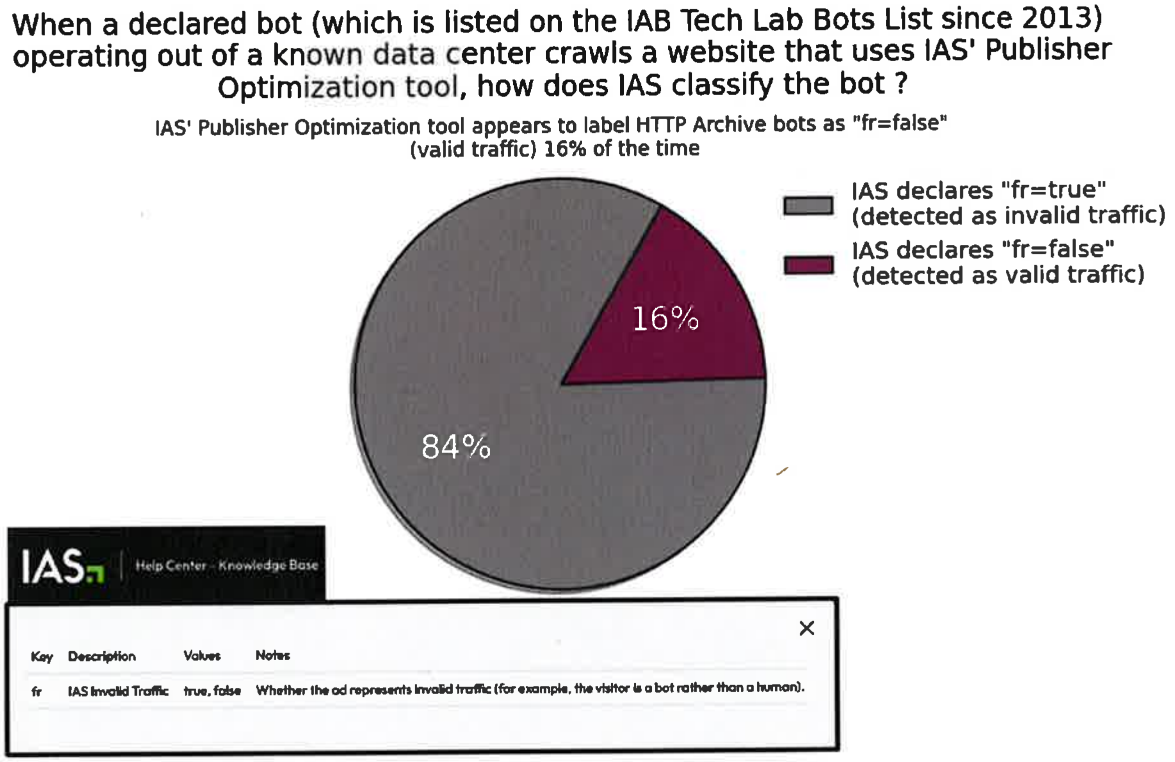
In addition to evaluating how IAS' publisher optimization tool classified URLScan.io's bots from 2019-2024, this study also examined how IAS classified HTTP Archive bots from 2022-2024. As mentioned earlier, HTTP Archive's bots openly declared themselves to be bots via the HTTP "User-Agent" request header. The HTTP Archive bot uses a User Agent string that has been on the IAB Tech Lab's Bots & Spiders list since 2013. This list is an industry resource compiled by the IAB Tech Lab, and various trade groups and accreditation bodies suggest that ad tech vendors utilize this reference list as a means of detecting and/or filtering out declared bot traffic. Furthermore, HTTP Archive's bots crawl the open from a set of publicly well known data center IP addresses.

Based on a sample of HTTP Archive crawls from 2022 to 2024 across over many distinct websites, it is possible to see how often IAS' Publisher Optimization tool labeled HTTP Archive's declared bot as "fr=true" (meaning, invalid traffic or a bot), versus "fr=false" (meaning, valid traffic or a human).

This dataset was compiled from instances where the declared HTTP Archive bot crawled many different websites, including fandom.com, usatoday.com, sky.it, cnn.com, wired.com, washingtonpost.com, weather.com, and others.

In some cases, IAS's Publisher Optimization tool correctly identified HTTP Archive's declared bot as a bot, and labeled it as "fr=true" (meaning its a bot and invalid traffic). In many cases however, URLScan.io's bot crawling a page was labeled as "fr=false" (valid, human traffic).

Across the sample of HTTP Archive crawls from 2022-2024, IAS's Publisher Optimization tool labeled the declared HTTP Archive bot (whose User Agent string has been on the IAB Tech Labs Bots & Spiders list since 2013) as "fr=false" (valid traffic or human) 16% of the time.

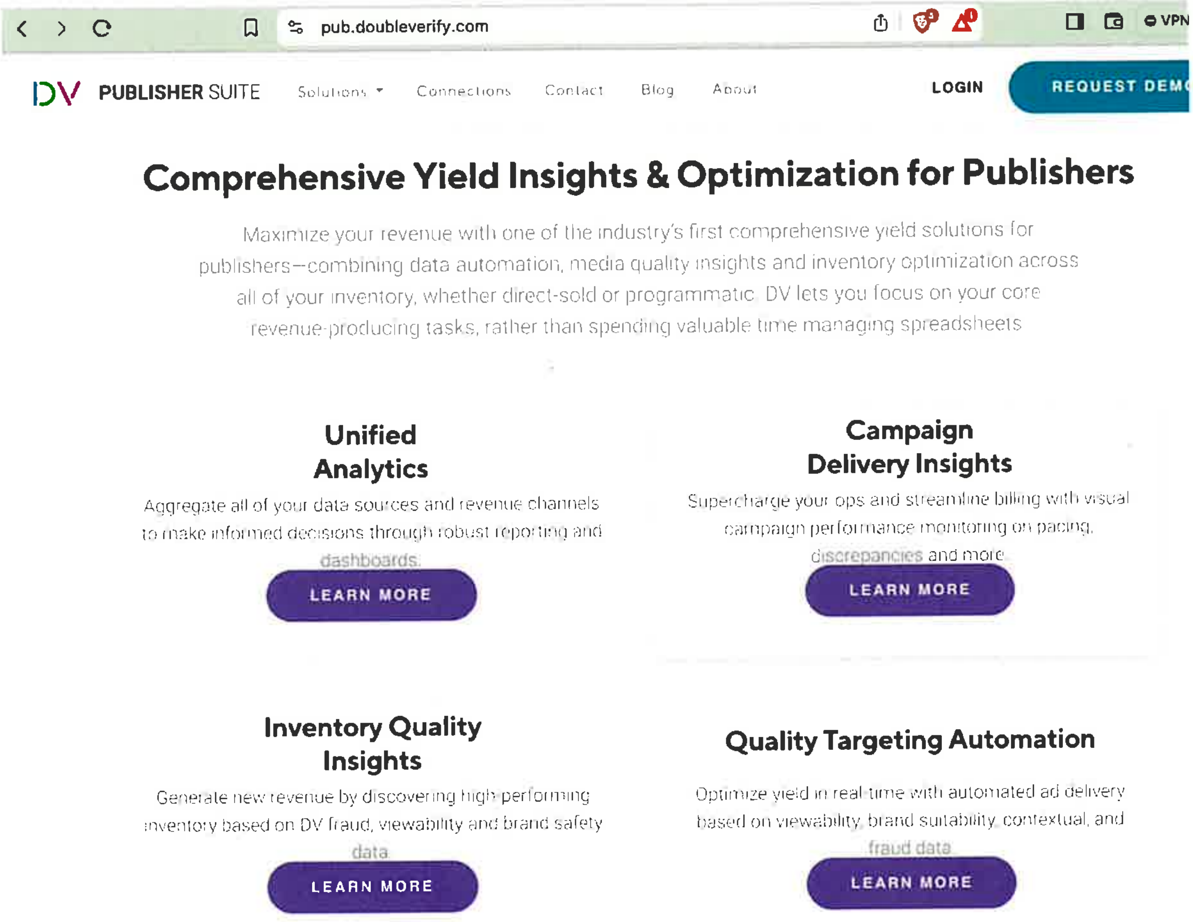


Key	Description	Values	Notes
fr	IAS Invalid Traffic	true, false	Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human).

For example, the HTTP Archive bot (which operates out of well known data center IP addresses and whose user agent has been on the IAB Tech Labs Bots & Spiders list since 2013) crawled washingtonpost.com every month from January 2022 to August 2024. The declared bot was classified as valid, human traffic ("fr=false") in March, April, May, July, August, and December of 2022, February, March, April, May, June, July, August, October, November, and December of 2023, and February, March, April, May, July, and August of 2024.

Research Results: Publishers which appear to partner with IAS and DoubleVerify and were seen serving ads to declared bots in data centers

Many publishers which appear to employ the IAS and DoubleVerify publisher optimization tools on their pages were observed serving ads to bots, including to declared bots operating out of known data center IP addresses, whose user agent has been on the IAB Tech Labs Bots & Spiders list since 2013.



Comprehensive Yield Insights & Optimization for Publishers

Maximize your revenue with one of the industry's first comprehensive yield solutions for publishers—combining data automation, media quality insights and inventory optimization across all of your inventory, whether direct-sold or programmatic. DV lets you focus on your core revenue-producing tasks, rather than spending valuable time managing spreadsheets

Unified Analytics

Aggregate all of your data sources and revenue channels to make informed decisions through robust reporting and dashboards.

LEARN MORE

Campaign Delivery Insights

Supercharge your ops and streamline billing with visual campaign performance monitoring on pacing, discrepancies and more.

LEARN MORE

Inventory Quality Insights

Generate new revenue by discovering high-performing inventory based on DV fraud, viewability and brand safety data.

LEARN MORE

Quality Targeting Automation

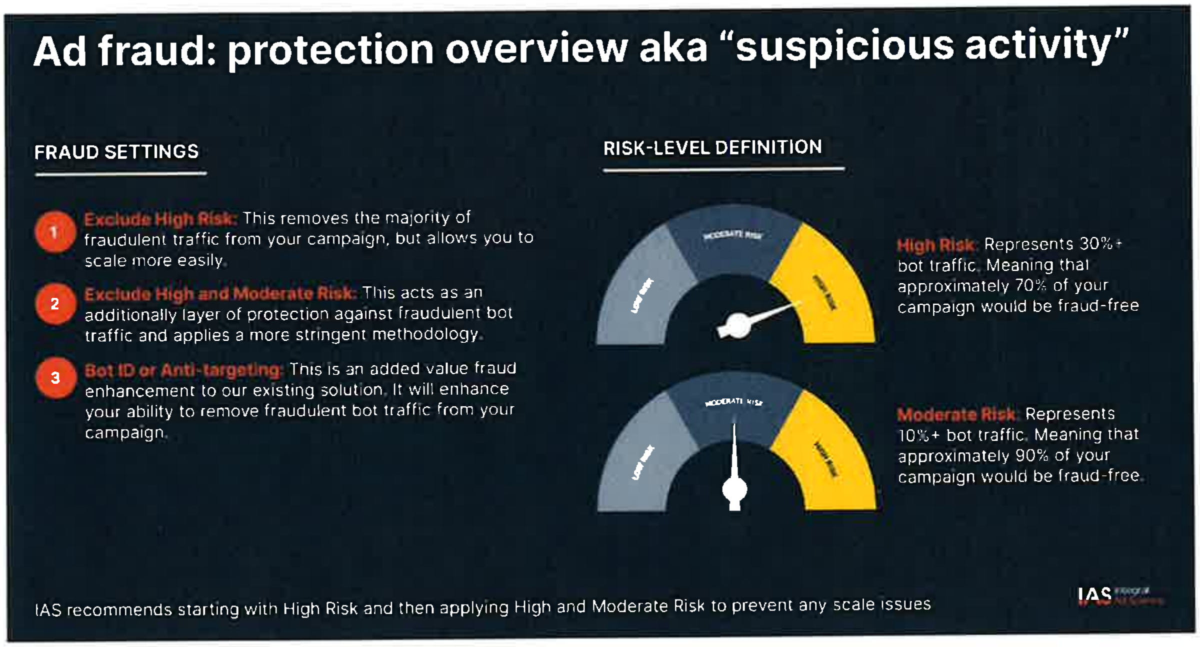
Optimize yield in real-time with automated ad delivery based on viewability, brand suitability, contextual, and fraud data.

LEARN MORE

Screenshot of DoubleVerify's website about its publisher optimization tool. Source: https://pub.doubleverify.com/

In some cases, even when one of the vendor's publisher optimization tools adjudicates that the given website visitor is a bot or invalid, fraudulent traffic, there are still ads being delivered to the bot. Some of those ads delivered to a bot after the bot was adjudicated to be bot traffic include references to IAS and DoubleVerify.

The publisher Trip Advisor appears to employ IAS' publisher optimization tool on its web pages. On April 23, 2023, URLScan.io's bot visited tripadvisor.com.sg, and the IAS publisher optimization tool (via endpoint "pixel.adsafeprotected.com/services/pub") was invoked by the publisher. The IAS API endpoint returned the classification "fr=true", indicating invalid, bot traffic. An ad for Air New Zealand was served to the bot by Trade Desk and Google. The source code of the Air New Zealand ad that was served to a bot after IAS's tool labeled the page view as "fr=true" indicated "charge-allIntegralSuspiciousActivity".



Ad fraud: protection overview aka "suspicious activity"

FRAUD SETTINGS

1. **Exclude High Risk:** This removes the majority of fraudulent traffic from your campaign, but allows you to scale more easily.
2. **Exclude High and Moderate Risk:** This acts as an additionally layer of protection against fraudulent bot traffic and applies a more stringent methodology.
3. **Bot ID or Anti-targeting:** This is an added value fraud enhancement to our existing solution. It will enhance your ability to remove fraudulent bot traffic from your campaign.

RISK-LEVEL DEFINITION

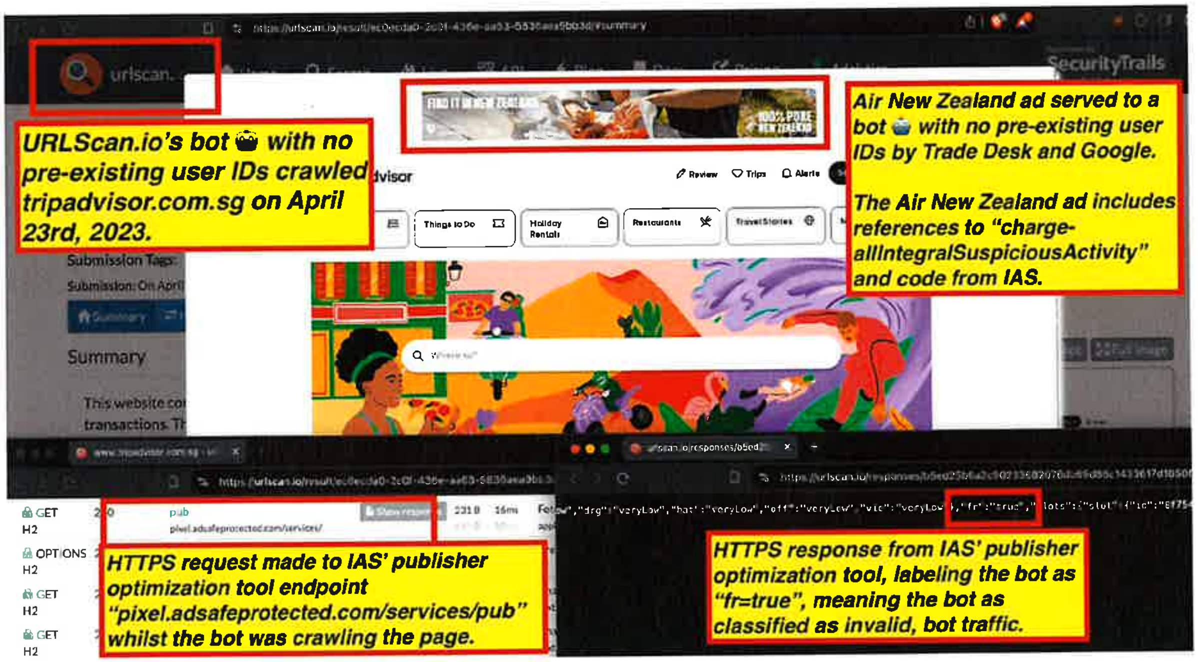
High Risk: Represents 30%+ bot traffic. Meaning that approximately 70% of your campaign would be fraud-free

Moderate Risk: Represents 10%+ bot traffic. Meaning that approximately 90% of your campaign would be fraud-free.

IAS recommends starting with High Risk and then applying High and Moderate Risk to prevent any scale issues

IAS

Screenshot of IAS technical documentation, describing IAS "Suspicious Activity" Pre-Bid Segments; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q



URLScan.io's bot 🤖 with no pre-existing user IDs crawled tripadvisor.com.sg on April 23rd, 2023.

Air New Zealand ad served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Google.

The Air New Zealand ad includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

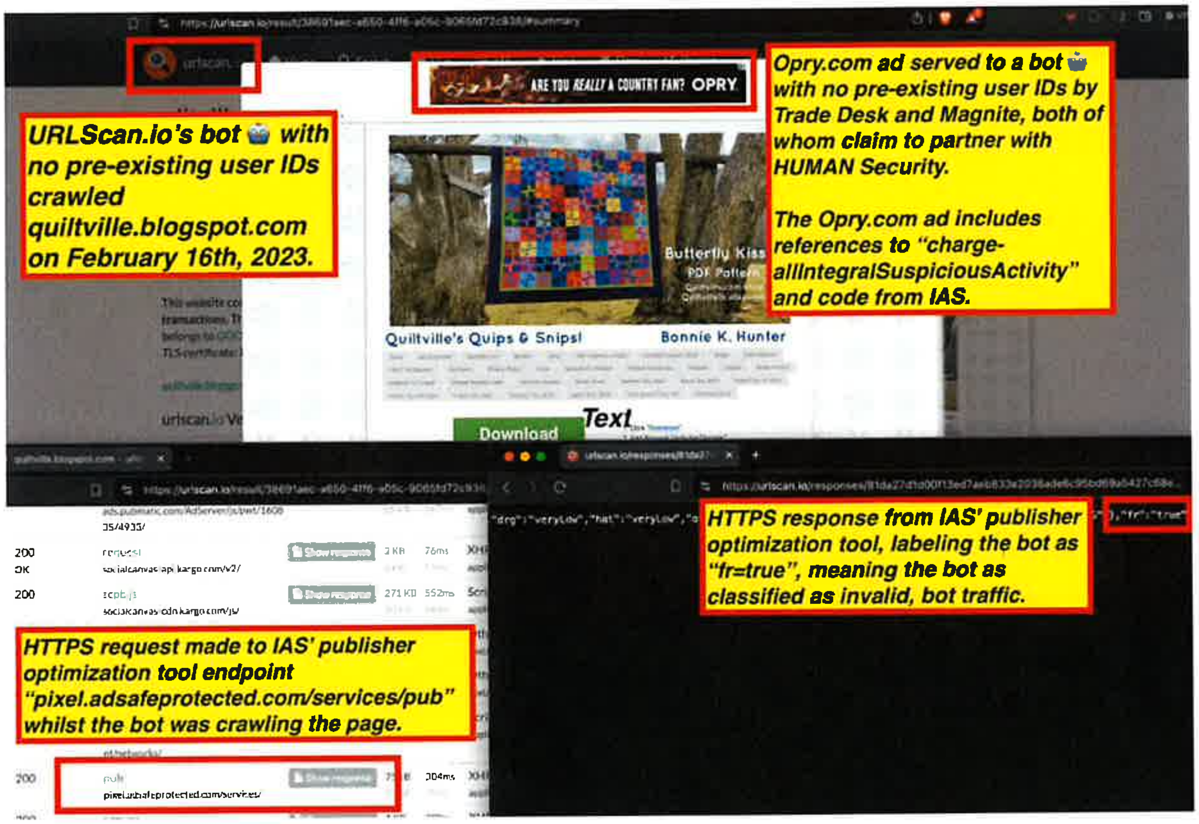
```
","drg":"veryLow","hat":"veryLow","off":"veryLow","vio":"veryLow"},"fr":"true","slots":{"slot":{"id":"Ef75
```

HTTPS request made to IAS' publisher optimization tool endpoint "pixel.adsafeprotected.com/services/pub" whilst the bot was crawling the page.

HTTPS response from IAS' publisher optimization tool, labeling the bot as "fr=true", meaning the bot as classified as invalid, bot traffic.

April 23, 2023, URLScan.io's bot visited tripadvisor.com.sg, and the IAS publisher optimization tool (via endpoint "pixel.adsafeprotected.com/services/pub") was invoked by the publisher. The IAS API endpoint returned the classification "fr=true", indicating invalid, bot traffic. An ad for Air New Zealand was served to the bot by Trade Desk and Google. The source code of the Air New Zealand ad that was served to a bot after IAS's tool labeled the page view as "fr=true" indicated "charge-allIntegralSuspiciousActivity". Source: https://urlscan.io/result/ec0ecda0-2c0f-436e-aa63-5836aea9bb3d/

As another example, on February 16th, 2023, URLScan.io's bot visited quiltville.blogspot.com, and the IAS publisher optimization tool (via endpoint "pixel.adsafeprotected.com/services/pub") was invoked. The IAS API endpoint returned the classification "fr=true", indicating invalid, bot traffic. An ad for Grand Ole Opry music stage in Nashville, Tennessee was served to the bot by Trade Desk and Magnite. The source code of the Opry ad that was served to a bot after IAS's tool labeled the page view as "fr=true" indicated "charge-allIntegralSuspiciousActivity".


urlscan
ARE YOU REALLY A COUNTRY FAN? OPRY
Butterfly Kiss
PDF Pattern
Quiltville's Quips & Snips!
Bonnie K. Hunter
Download
Text
"drg":"veryLow","hat":"veryLow"
"fr":"true"

URLScan.io's bot 🤖 with no pre-existing user IDs crawled quiltville.blogspot.com on February 16th, 2023.

Opry.com ad served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.

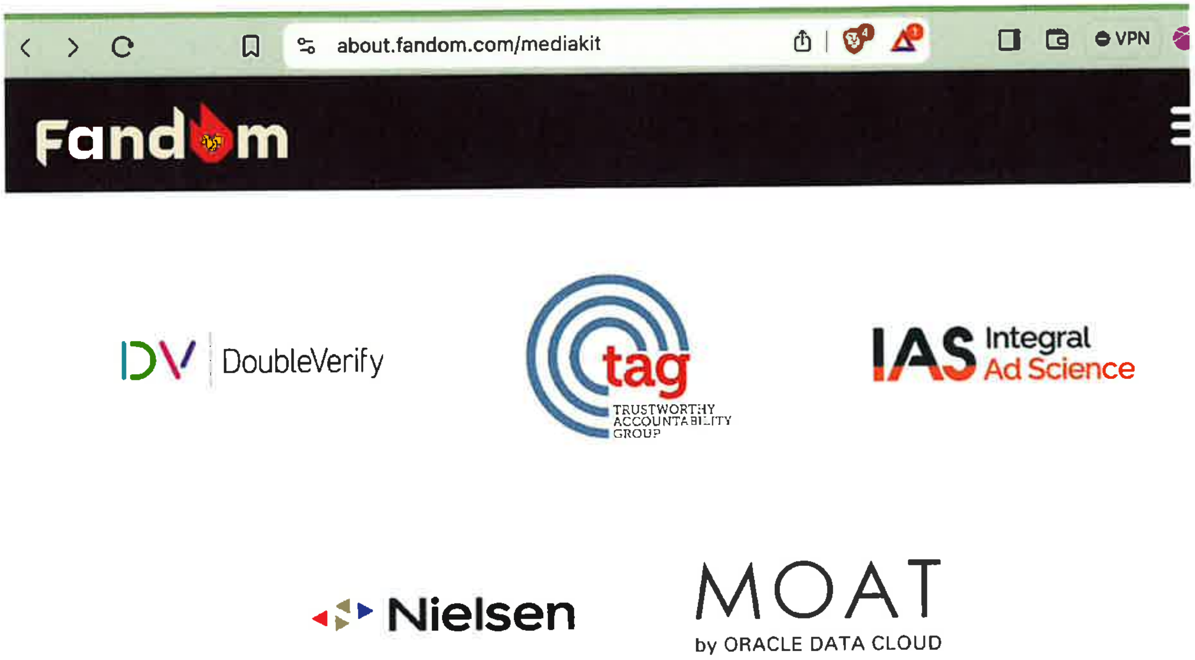
The Opry.com ad includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

HTTPS response from IAS' publisher optimization tool, labeling the bot as "fr=true", meaning the bot as classified as invalid, bot traffic.

HTTPS request made to IAS' publisher optimization tool endpoint "pixel.adsafeprotected.com/services/pub" whilst the bot was crawling the page.

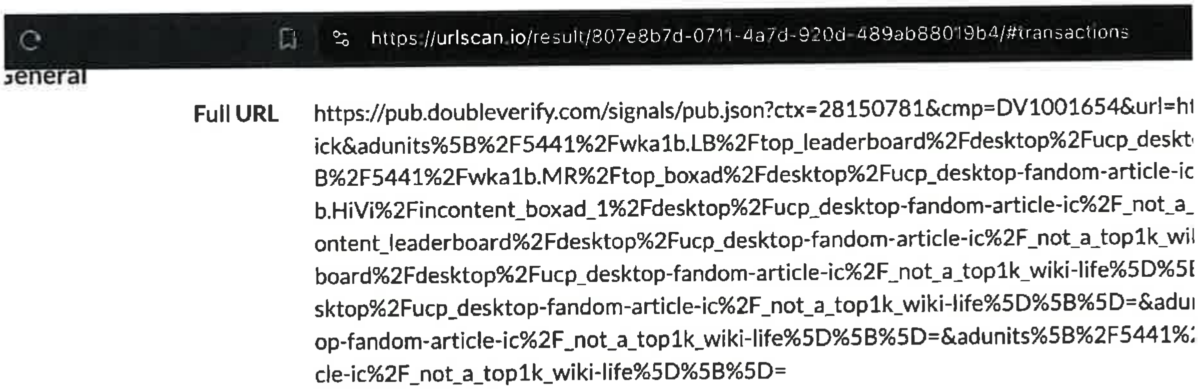
On February 16th, 2023, URLScan.io's bot visited quiltville.blogspot.com, and the IAS publisher optimization tool (via endpoint "pixel.adsafeprotected.com/services/pub") was invoked.. The IAS API endpoint returned the classification "fr=true", indicating invalid, bot traffic. An ad for Grande Ole Opry music stage in Nashville, Tennessee was served to the bot by Trade Desk and Magnite. The source code of the Opry ad that was served to a bot after IAS's tool labeled the page view as "fr=true" indicated "charge-allIntegralSuspiciousActivity". Source: https://urlscan.io/result/38691aec-a650-4ff6-a05c-9065fd72c938/#summary

For example, the website fandom.com appears to utilize pre-auction publisher optimization code from both IAS and DoubleVerify. Fandom.com's media kit lists both vendors as "partners".



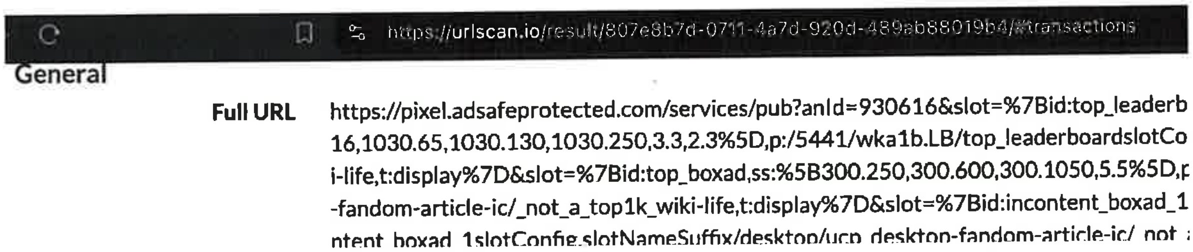
Source: Fandom media kit - https://perma.cc/DCP2-FASY

URLScan.io's bot crawled icehockey.fandom.com on December 24th, 2023 with no pre-existing user IDs from a data center in Australia. One can see that DoubleVerify and IAS' publisher optimization code was invoked whilst the bot was crawling the fandom.com page.


https://urlscan.io/result/807e8b7d-0711-4a7d-920d-489ab88019b4/#transactions

General

Full URL https://pub.doubleverify.com/signals/pub.json?ctx=28150781&cmp=DV1001654&url=ht
ick&adunits%5B%2F5441%2Fwka1b.LB%2Ftop_leaderboard%2Fdesktop%2Fucp_deskt
B%2F5441%2Fwka1b.MR%2Ftop_boxad%2Fdesktop%2Fucp_desktop-fandom-article-ic
b.HiVi%2Fincontent_boxad_1%2Fdesktop%2Fucp_desktop-fandom-article-ic%2F_not_a_
ontent_leaderboard%2Fdesktop%2Fucp_desktop-fandom-article-ic%2F_not_a_top1k_wi
board%2Fdesktop%2Fucp_desktop-fandom-article-ic%2F_not_a_top1k_wiki-life%5D%5
sktop%2Fucp_desktop-fandom-article-ic%2F_not_a_top1k_wiki-life%5D%5B%5D=&adu
op-fandom-article-ic%2F_not_a_top1k_wiki-life%5D%5B%5D=&adunits%5B%2F5441%
cle-ic%2F_not_a_top1k_wiki-life%5D%5B%5D=



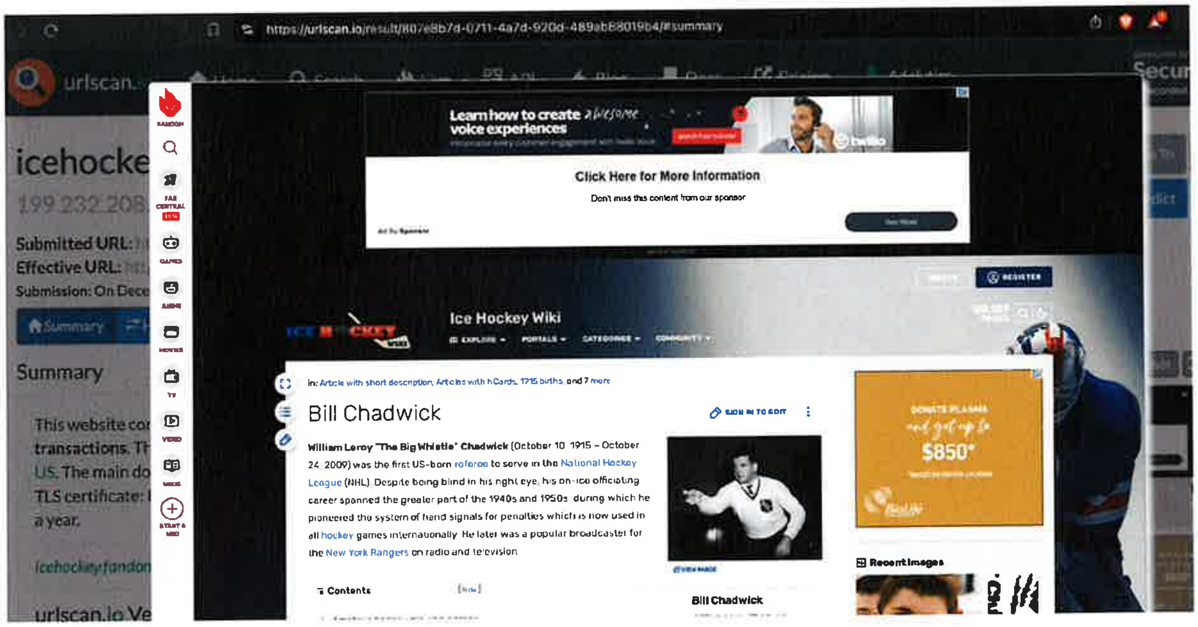
https://urlscan.io/result/807e8b7d-0711-4a7d-920d-489ab88019b4/#transactions

General

Full URL https://pixel.adsafeprotected.com/services/pub?anId=930616&slot=%7Bid:top_leaderb
16,1030.65,1030.130,1030.250,3.3,2.3%5D,p:/5441/wka1b.LB/top_leaderboardslotCo
i-life,t:display%7D&slot=%7Bid:top_boxad,ss:%5B300.250,300.600,300.1050,5.5%5D,p
-fandom-article-ic/_not_a_top1k_wiki-life,t:display%7D&slot=%7Bid:incontent_boxad_1
ntent_boxad_1slotConfig.slotNameSuffix/desktop/ucp_desktop-fandom-article-ic/_not_

Screenshot showing an HTTP request to pub.doubleverify.com/signals/pub.json and pixel.adsafeprotected.com/services/pub made on fandom.com whilst URLScan.io's bot was crawling the page. Source: https://urlscan.io/result/807e8b7d-0711-4a7d-920d-489ab88019b4/#transactions

The bot was served an ad from BioLife Plasma Services, transacted via Trade Desk and Microsoft Xandr SSP. The source code of the BioLife Plasma ad includes references to and code from DoubleVerify.



https://urlscan.io/result/807e8b7d-0711-4a7d-920d-489ab88019b4/#summary

in: Article with short description, Articles with hCards, 1915 births, and 7 more

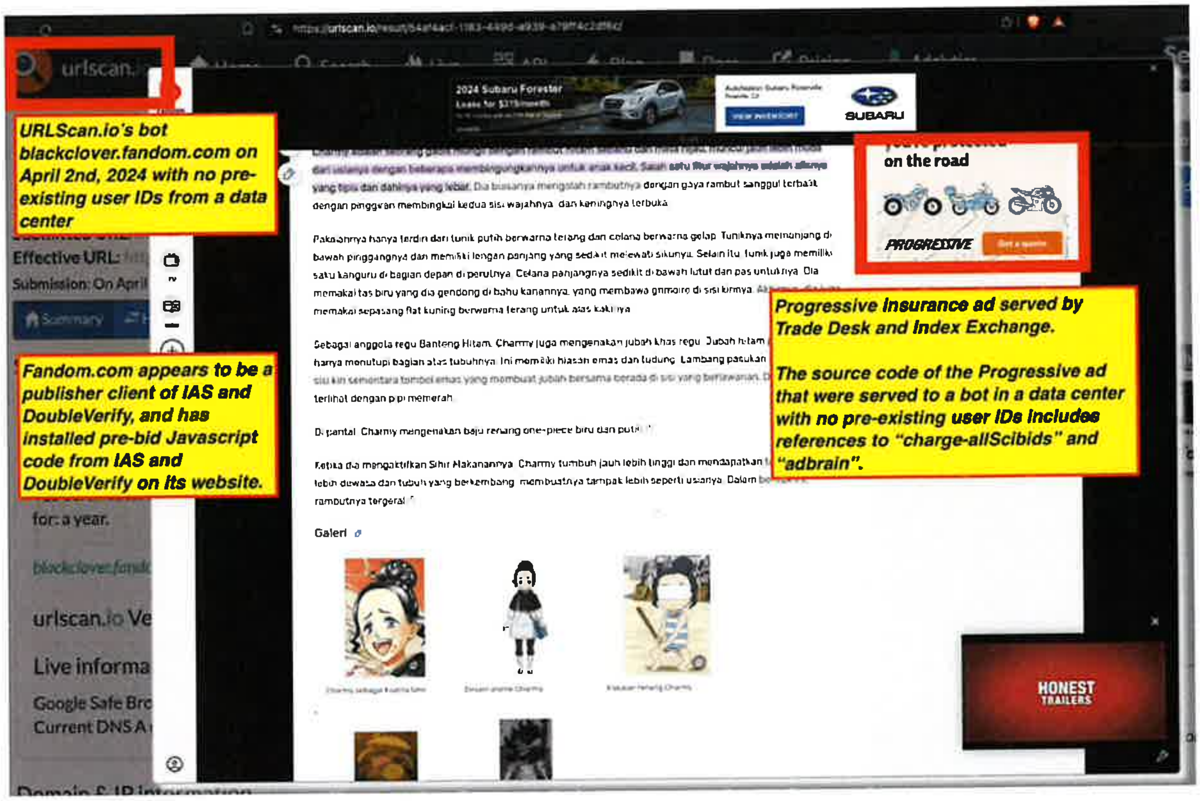
Bill Chadwick

William Leroy "The Big Whistle" Chadwick (October 10, 1915 – October 24, 2009) was the first US-born referee to serve in the National Hockey League (NHL). Despite being blind in his right eye, his on-ice officiating career spanned the greater part of the 1940s and 1950s, during which he pioneered the system of hand signals for penalties which is now used in all hockey games internationally. He later was a popular broadcaster for the New York Rangers on radio and television.

Screenshot of a BioLife Plasma Services ad served to URLScan.io's bot whilst the bot was crawling fandom.com. Source: https://urlscan.io/result/807e8b7d-0711-4a7d-920d-489ab88019b4/#summary

As another example, URLScan.io's bot crawled blackclover.fandom.com on April 2nd, 2024 with no pre-existing user IDs. One can see that

DoubleVerify and IAS' publisher optimization code was invoked whilst the bot was crawling the fandom.com page. The bot was then served an ad for Progressive insurance by Trade Desk and Index Exchange. The source code of the Progressive insurance ads includes references to "charge-allScibids".


URLScan.io's bot blackclover.fandom.com on April 2nd, 2024 with no pre-existing user IDs from a data center

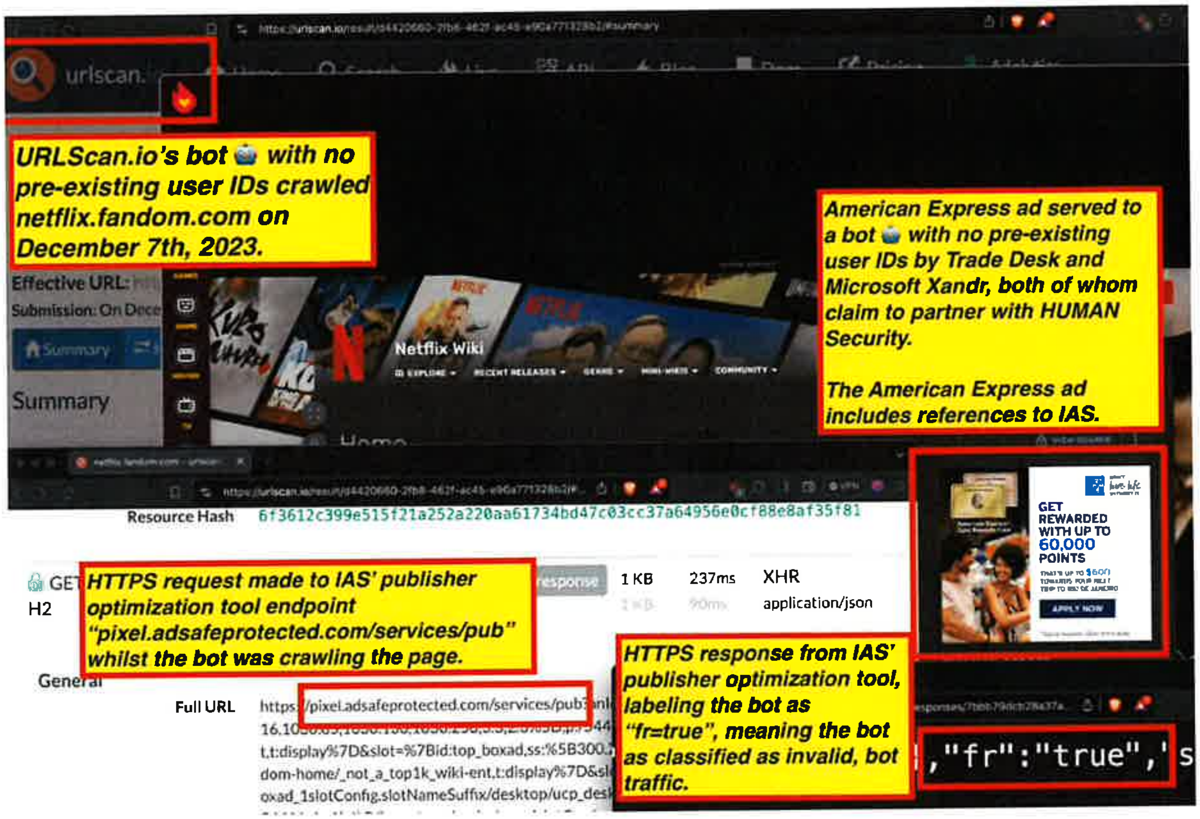
Fandom.com appears to be a publisher client of IAS and DoubleVerify, and has installed pre-bid Javascript code from IAS and DoubleVerify on its website.

Progressive Insurance ad served by Trade Desk and Index Exchange.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain".

Screenshot of URLScan.io's bot crawling blackclover.fandom.com on April 2nd, 2024 whilst being shown a Progressive insurance ad that contains references to "charge-allScibids" and "adbrain". The publisher fandom.com appears to have configured the IAS and DoubleVerify publisher optimization tools on its website, and lists IAS and DoubleVerify as "partners" in its media kit for prospective advertisers. Source: https://urlscan.io/result/54af4acf-1183-449d-a939-a79ff4c2df6c/

As another example, URLScan.io's bot crawled nextflix.fandom.com on December 7th, 2023. Fandom.com's page invoked both the IAS and DoubleVerify publisher optimization tools. The IAS publisher optimization tool returned the classification "fr=true", indicating invalid, bot traffic. An ad for American Express was served to the bot by Trade Desk and Microsoft Xandr. The American Express ad included references to IAS.



URLScan.io's bot with no pre-existing user IDs crawled netflix.fandom.com on December 7th, 2023.

American Express ad served to a bot with no pre-existing user IDs by Trade Desk and Microsoft Xandr, both of whom claim to partner with HUMAN Security.

The American Express ad includes references to IAS.

Resource Hash 6f3612c399e515f21a252a220aa61734bd47c03cc37a64956e0cf88e8af35f81

HTTPS request made to IAS' publisher optimization tool endpoint "pixel.adsafeprotected.com/services/pub" whilst the bot was crawling the page.

1 KB 237ms XHR application/json

Full URL https://pixel.adsafeprotected.com/services/pub
t,t:display%7D&slot=%7Bid:top_boxad,ss:%5B300
dom-home/_not_a_top1k_wiki-ent,t:display%7D&sl
oxad_1slotConfig.slotNameSuffix/desktop/ucp_des

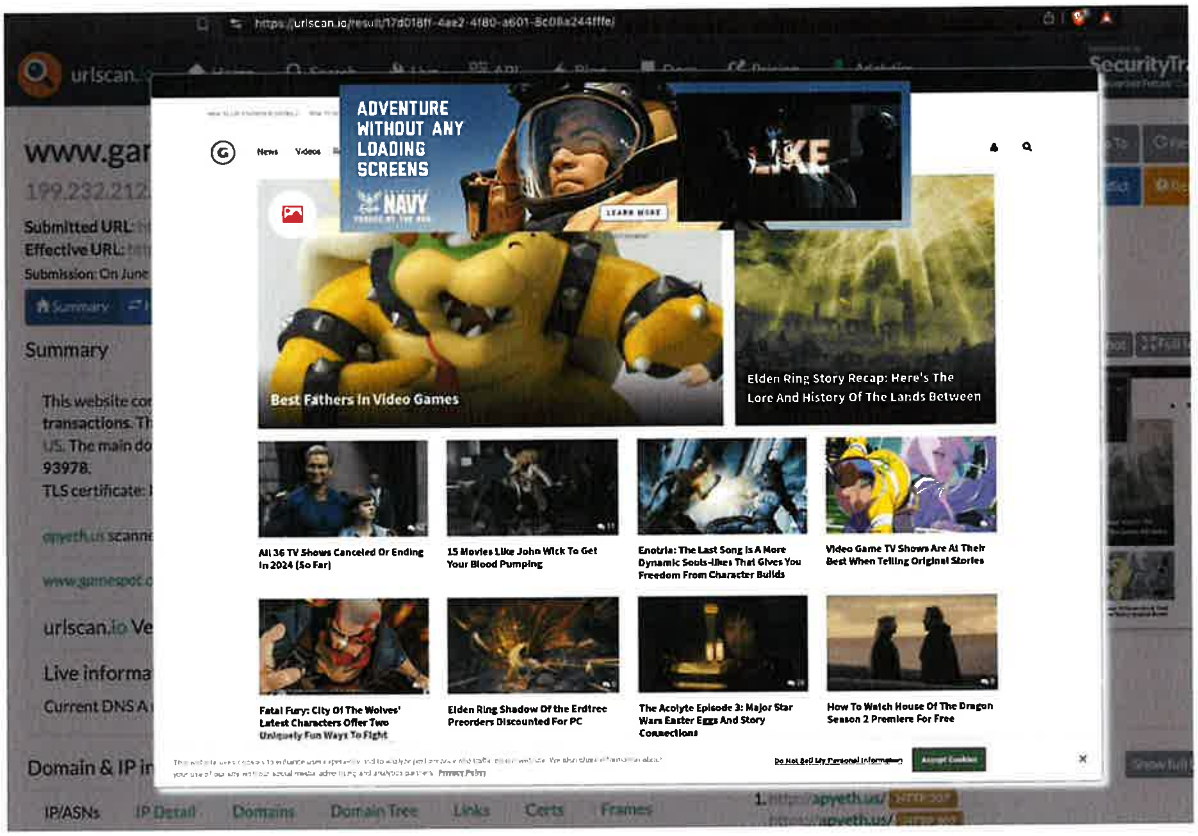
HTTPS response from IAS' publisher optimization tool, labeling the bot as "fr=true", meaning the bot as classified as invalid, bot traffic.

```
,"fr":"true",'
```

Screenshot of an American Express ad served to URLScan.io's bot. DoubleVerify and IAS' publisher optimization tools were invoked by the publisher fandom.com. The IAS publisher optimization tool labeled the session as "fr=true", indicating invalid, bot traffic. Source: https://urlscan.io/result/d4420660-2fb8-462f-ac45-e90a771328b2/#summary

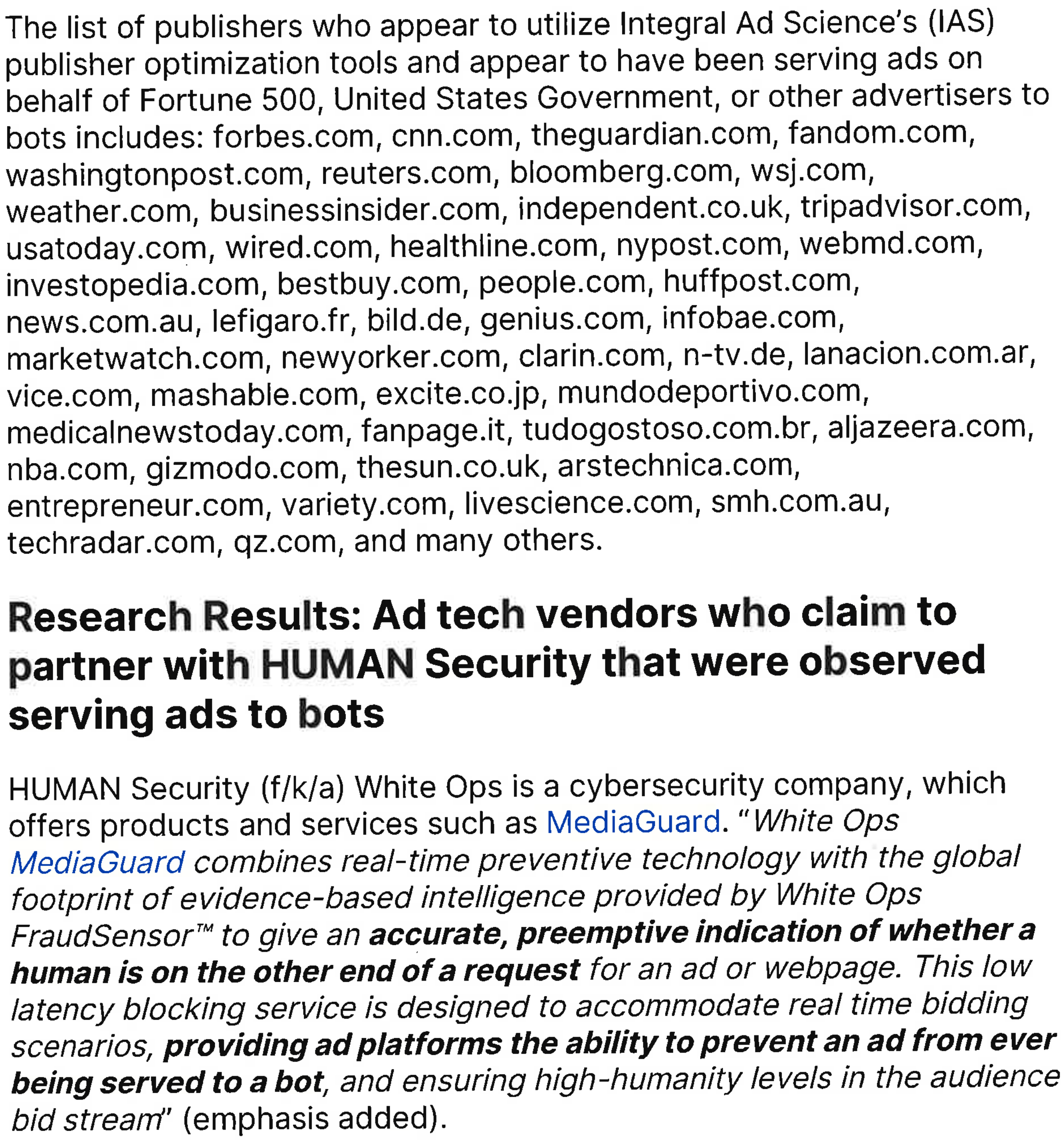
As another example, URLScan.io's bot crawled timeout.com on May 20th, 2024. The publisher timeout.com invoked the DoubleVerify publisher tool by making an HTTPS request to "pub.doubleverify.com/signals/pub.json". Afterwards, an ad for the National Football League (NFL) was served to the bot via Trade Desk and ShareThrough SSP. The source code of the NFL ad appeared to contain code from DoubleVerify and references to "charge-allDoubleVerifyBotAvoidance".

As another example. United States Navy ads were served to URLScan.io's bot whilst the bot was crawling fandom.com, which uses both IAS and DoubleVerify publisher optimization tools on its web pages.


https://urlscan.io/result/17d018ff-4ae2-4180-a601-8c08a244fffe/
urlscan
SecurityTr
www.gar
199.232.212
Submitted URL:
Effective URL:
Submission: On June
Summary
Summary
This website co
transactions. Th
US. The main do
93978.
TLS certificate:
apyeth.us scann
www.gamespot.c
urlscan.io Ve
Live informa
Current DNS A
Domain & IP in
IP/ASNs
IP Detail
Domains
Domain Tree
Links
Certs
Frames
1. https://apyeth.us/
https://apyeth.us/
News
Videos
ADVENTURE WITHOUT ANY LOADING SCREENS
NAVY
LEARN MORE
LIKE
Best Fathers In Video Games
Elden Ring Story Recap: Here's The Lore And History Of The Lands Between
All 36 TV Shows Canceled Or Ending In 2024 (So Far)
15 Movies Like John Wick To Get Your Blood Pumping
Enotria: The Last Song Is A More Dynamic Souls-like That Gives You Freedom From Character Builds
Video Game TV Shows Are At Their Best When Telling Original Stories
Fatal Fury: City Of The Wolves' Latest Characters Offer Two Uniquely Fun Ways To Fight
Elden Ring Shadow Of the Erdtree Preorders Discounted For PC
The Acolyte Episode 3: Major Star Wars Easter Eggs And Story Connections
How To Watch House Of The Dragon Season 2 Premiere For Free
Do Not Sell My Personal Information
Accept Cookies
Privacy Policy

The list of publishers who appear to utilize DoubleVerify's publisher optimization tools and appear to have been serving ads on behalf of Fortune 500, United States Government, or other advertisers to bots includes: forbes.com, bbc.com, telegraph.co.uk, bloomberg.com, weather.com, businessinsider.com, independent.co.uk, cnbc.com, globo.com, time.com, healthline.com, cnet.com, mayoclinic.org, buzzfeed.com, newsweek.com, webmd.com, sapo.pt, theverge.com, nbcnews.com, fandom.com, elpais.com, theatlantic.com, huffpost.com, realtor.com, economist.com, infobae.com, sportskeeda.com, goal.com, clarin.com, n-tv.de, target.com, zdnet.com, mashable.com, fastcompany.com, medicalnewstoday.com, futbin.com, g1.globo.com, kooora.com, arca.live, vox.com, ge.globo.com, inc.com, ign.com, bizjournals.com, pcmag.com, euronews.com, today.com, thedailybeast.com, lifehacker.com, and many others.

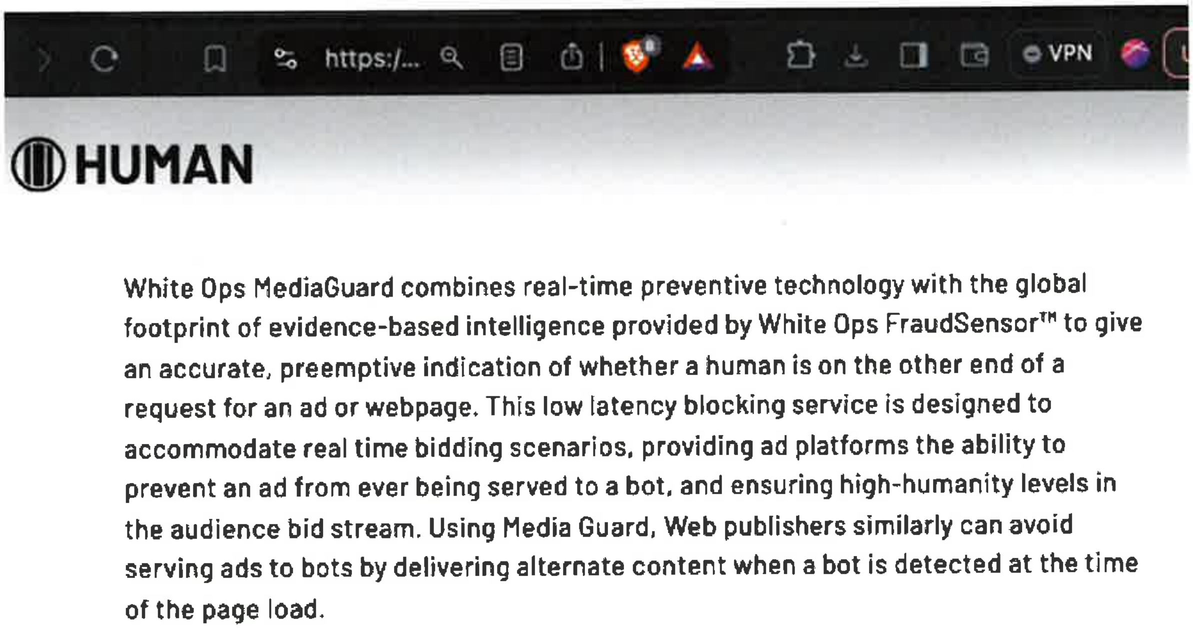
https://adalytics.io/blog/prebid-bot-filtration



The list of publishers who appear to utilize Integral Ad Science's (IAS) publisher optimization tools and appear to have been serving ads on behalf of Fortune 500, United States Government, or other advertisers to bots includes: forbes.com, cnn.com, theguardian.com, fandom.com, washingtonpost.com, reuters.com, bloomberg.com, wsj.com, weather.com, businessinsider.com, independent.co.uk, tripadvisor.com, usatoday.com, wired.com, healthline.com, nypost.com, webmd.com, investopedia.com, bestbuy.com, people.com, huffpost.com, news.com.au, lefigaro.fr, bild.de, genius.com, infobae.com, marketwatch.com, newyorker.com, clarin.com, n-tv.de, lanacion.com.ar, vice.com, mashable.com, excite.co.jp, mundodeportivo.com, medicalnewstoday.com, fanpage.it, tudogostoso.com.br, aljazeera.com, nba.com, gizmodo.com, thesun.co.uk, arstechnica.com, entrepreneur.com, variety.com, livescience.com, smh.com.au, techradar.com, qz.com, and many others.

Research Results: Ad tech vendors who claim to partner with HUMAN Security that were observed serving ads to bots

HUMAN Security (f/k/a) White Ops is a cybersecurity company, which offers products and services such as MediaGuard. "*White Ops MediaGuard combines real-time preventive technology with the global footprint of evidence-based intelligence provided by White Ops FraudSensor™ to give an* ***accurate, preemptive indication of whether a human is on the other end of a request*** *for an ad or webpage. This low latency blocking service is designed to accommodate real time bidding scenarios,* ***providing ad platforms the ability to prevent an ad from ever being served to a bot****, and ensuring high-humanity levels in the audience bid stream*" (emphasis added).



White Ops MediaGuard combines real-time preventive technology with the global footprint of evidence-based intelligence provided by White Ops FraudSensor™ to give an accurate, preemptive indication of whether a human is on the other end of a request for an ad or webpage. This low latency blocking service is designed to accommodate real time bidding scenarios, providing ad platforms the ability to prevent an ad from ever being served to a bot, and ensuring high-humanity levels in the audience bid stream. Using Media Guard, Web publishers similarly can avoid serving ads to bots by delivering alternate content when a bot is detected at the time of the page load.

Source: HUMAN Security website

Which demand side platforms (DSPs) were observed transacting the highest relative number of ad impressions to bots in Oct 2024?

A preliminary research question was to determine which demand side platforms (DSPs) or ad software used for purchasing ads by media buyers appeared to transact the highest number of ad impressions to bots in a specific time frame.

To approach this question, data from URLScan.io and from HTTP Archive was analyzed for the month of October 2024.

URLScan.io and HTTP Archive's crawl dataset records were queried for a number of demand side platform "selectors". A "selector" is a term of art commonly used by signals intelligence (SIGINT) professionals working at the National Security Agency (NSA), Government Communications Headquarters (GCHQ), or Unit 8200 of the Israel Defense Forces.

According to the Director of National Intelligence (ODNI), a "selector" is a "unique identifier" associated with a target of interest. For example, a telephone number or email address can be a selector used to parse large amounts of raw signals intelligence data when trying to track a specific target as part of a foreign intelligence operation.

In this present context, "selector" refers to an identifier that can unambiguously confirm that a specific ad tech provider transacted a given ad. For example, ads transacted to a bot by the Trade Desk DSP contain win notification pixels from endpoints such as "vam-bid.adsrvr.org/bid/feedback/". Ads transacted to a bot by Freewheel Beeswax DSP contain a win notification pixels from endpoints such as "us-east-1.event.prod.bidr.io/log/imp/". Ads transacted to a bot by Yahoo DSP contain win notification pixels such as: "pn.ybp.yahoo.com/ab/secure/true/imp/".

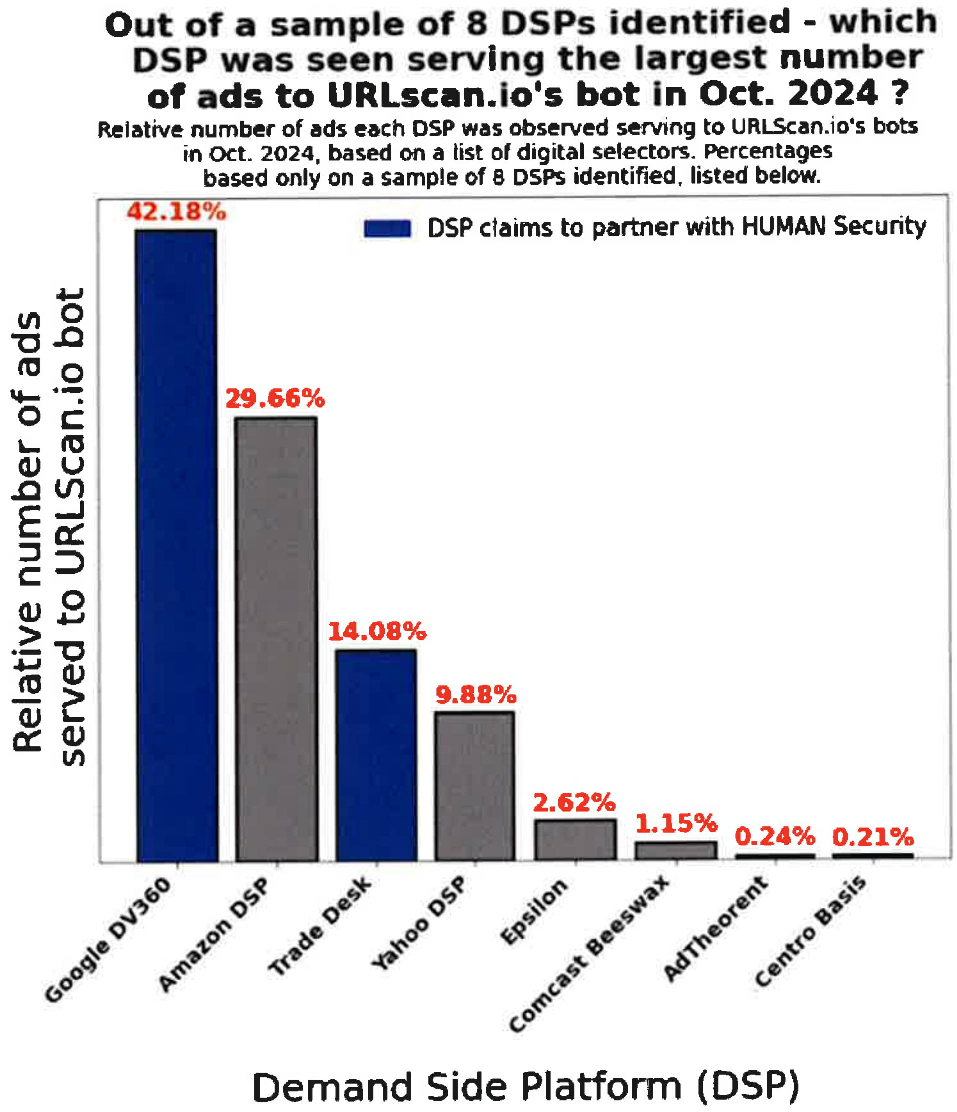
Data from URLScan.io and from HTTP Archive's bot crawl session from October 2024 was filtered and counted for the presence of various DSP specific selectors.

Eight (8) demand side platforms (DSPs) were analyzed during the course of this exploratory analysis, including:

1. Google Display & Video 360 (DV360)
2. Amazon DSP
3. Trade Desk DSP
4. Yahoo DSP
5. Epsilon ad buying platform (distinct from Epsilon Conversant SSP)
6. Comcast Freewheel Beeswax
7. AdTheorent
8. Basis Technologies (f/k/a Centro)

Based on analysis of URLScan.io data from October 2024, it appears that DV360 transacted the highest number of ad impressions to URLScan.io's bots, as determined by the presence of DV360 related ad selectors. Amazon DSP transacted the second highest number of ads to URLScan.io's bot, and Trade Desk transacted the third highest number of ads to URLScan.io's bots in the October 2024 sample.

It bears mentioning that this sample was not normalized or adjusted by market adoption or utilization rates of each DSP. The fact that DV360 or Amazon were observed serving such a relatively high number of ads to bots when compared to other DSPs such as Yahoo DSP may simply be a function of DV360 or Amazon having more market adoption and transacting a higher volume of ad impressions each month than Yahoo DSP. Readers are strongly encouraged to be careful when analyzing this sample of data and considering various artifacts which may have affected the sample results



It bears mentioning that two of the DSPs or ad bidding platforms references above - Google DV360 and Trade Desk - claim to partner with HUMAN Security for invalid traffic (IVT) detection. HUMAN Security possesses various Media Rating Council (MRC) certifications related to bot filtration as well as being TAG Certified Against Fraud.

In addition to examining a sample of data from URLScan.io, data from the HTTP Archive bot was also examined to see how many ads were served to this second bot by various ad tech vendors.

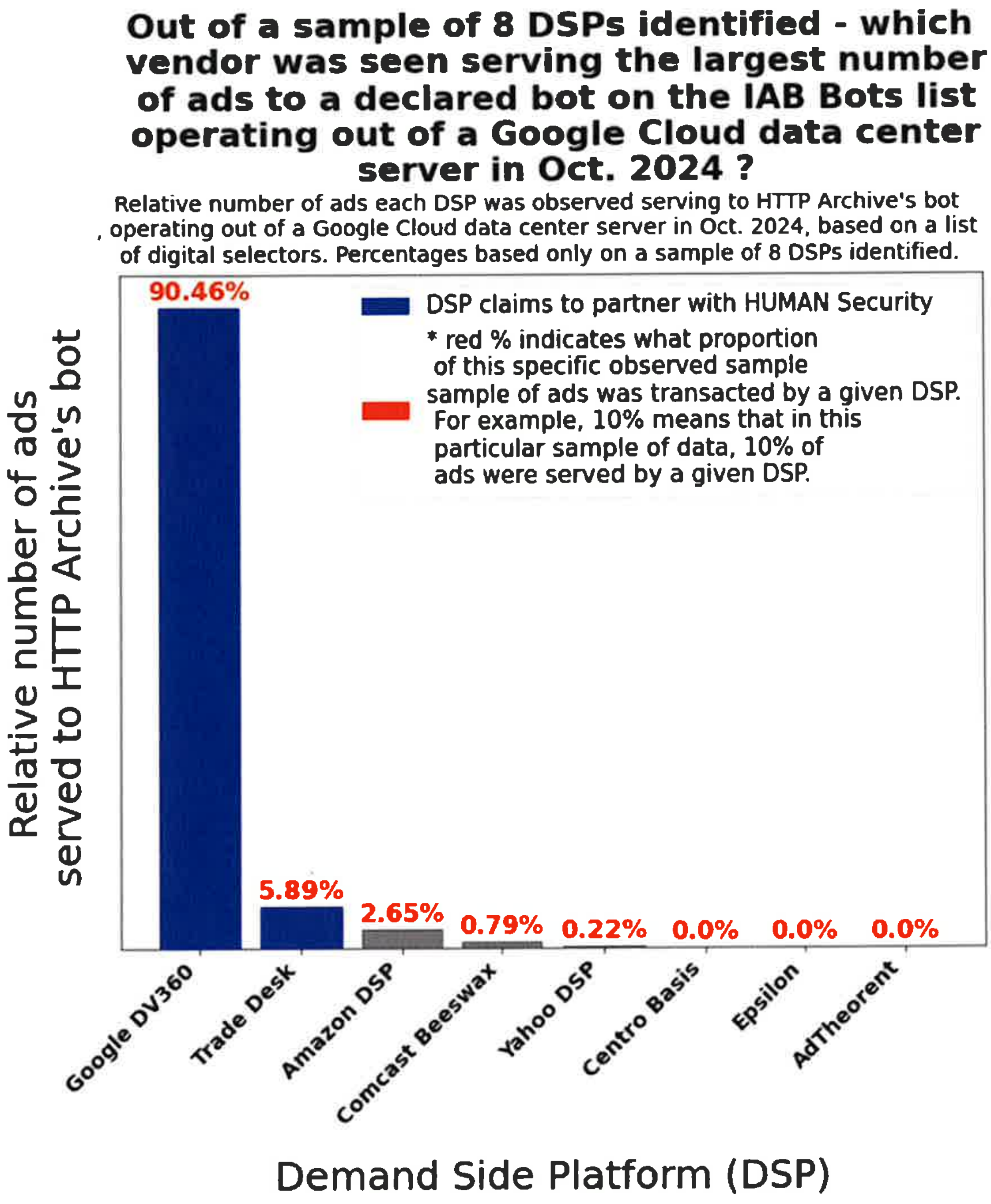
It bears mentioning that HTTP Archive's bot is a declared bot whose user agent has been on the IAB Tech Lab's Bots & Spiders List since 2013. Furthermore, the HTTP Archive bot crawls the web from known Google Cloud data center IPs, some of which may be on industry data center lists.

The HTTP Archive data was similarly analyzed for October 2024. The data was filtered and counted for the presence of various DSP selectors to determine how many ads a given vendor had transacted with HTTP Archive's bot.

Some ad tech vendors, such as Ad Theorent, Basis Technologies, and Epsilon (demand side) were not observed transacting any ad impressions to HTTP Archive's declared bot.

Google DV360 was observed serving far more ads than any other vendor in this sample. This may be counter-intuitive, as Google presumably has full awareness of which IP addresses are known Google Cloud data center IPs and might be able to easily filter out bot traffic from its own data centers from being served digital ads by its platforms.

Google DV360 was observed transacting about ~15x times as many ads to a declared bot operating out of a Google data center as the Trade Desk. Both Google DV360 and Trade Desk claim to partner with HUMAN Security for bot filtering. It bears noting that even though the two DSPs that have issued public statements about claiming to partner with HUMAN Security were observed serving the highest number of ads to a declared bot on the IAB Bots & Spiders List operating out of a known data center IP, this may be a function of how much market share these two DSPs have relative to other DSPs. This analysis does not "normalize" or account for relative market share or total volume of impressions each DSP transacted each month.



As mentioned above, it is worth noting that some demand side platforms - such as Basis Technologies (f/k/a as Centro) - were not observed transacting any ad impressions to HTTP Archive's bot in October 2024.

Prompted by these observations, Adalytics reached out to some of the demand side platforms (DSPs) who appear to be filtering out declared bot traffic. Adalytics asked them for comments about how and why they are filtering out declared bot traffic, or preventing ads from serving to declared bots such as the HTTP Archive bot.

Basis Technologies (f/k/a Centro) agreed to provide comments “on the record” that could be cited in this report.

Adalytics asked:

“What is Basis Technologies' philosophy about serving ads to declared bots operating out of known data center IPs? Should DSPs filter out and avoid bidding on ad auctions served to declared bots on the IAB Bots & Spiders List operating out of known data center IPs? What is Basis Technologies’ technical approach to ensuring that no ads were seen serving to a declared bot in Oct 2024 from [HTTP Archive] ?'

Chris Coupland, Basis Technologies’ platform operations director, responded:

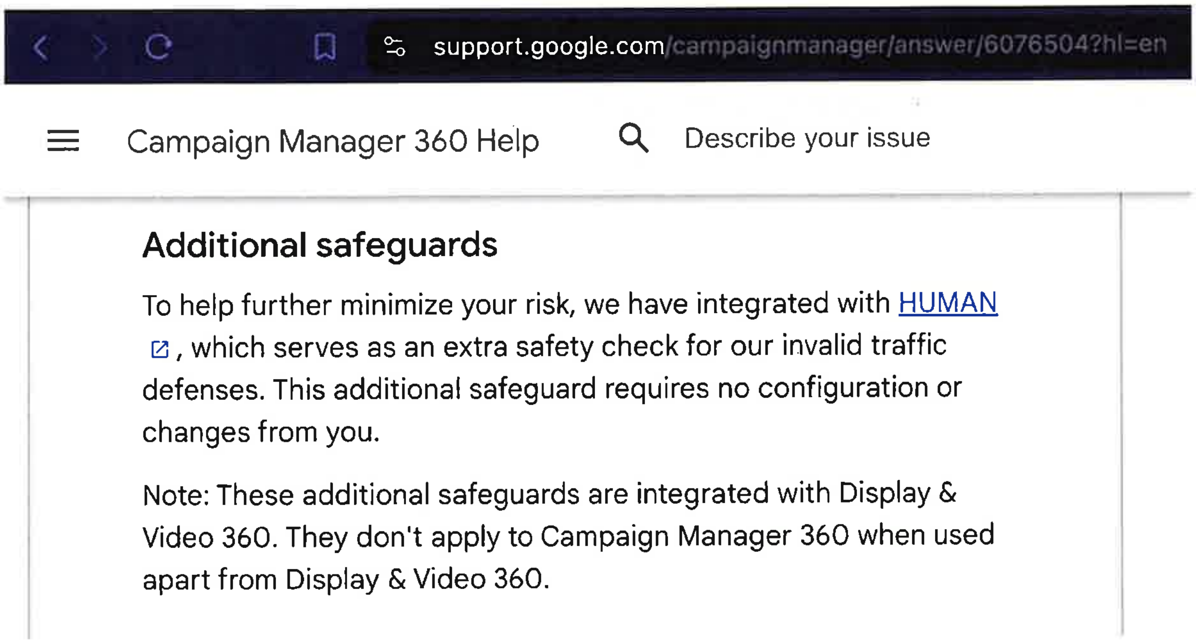
“Basis strives to remove all invalid traffic (IVT) as per MRC guidelines, which requires ad tech vendors that measure advertising traffic to filter it from their reporting. Basis will not bid on impressions deemed to be IVT. The most basic form of this, general invalid traffic (GIVT), consists of the type referenced -- traffic originating in datacenters, user agents declared in the IAB's Spiders and Bots list, unknown user agents, etc.

Basis employs multiple methods of filtering or blocking GIVT. We maintain blocklists of known datacenter IP addresses, sourced from multiple vendors, and actively enforce the IAB's Spiders and Bots list. We’ve had these methods in place for many years and are why the 'academic bot' doesn't show up in Adalytics reporting.”

The next two sections of this report will go into greater detail of how the two demand side platforms that claim to partner with HUMAN Security - Google DV360 and Trade Desk - were observed serving ads for many US Government and Fortune 500 advertisers to bots.

Google DV360 ads served to bots

According to Google's public documentation, Google has "*integrated with HUMAN, which serves as an extra safety check for our invalid traffic defenses. This additional safeguard requires no additional configuration or changes from you.*"


support.google.com/campaignmanager/answer/6076504?hl=en
Campaign Manager 360 Help
Describe your issue

Additional safeguards

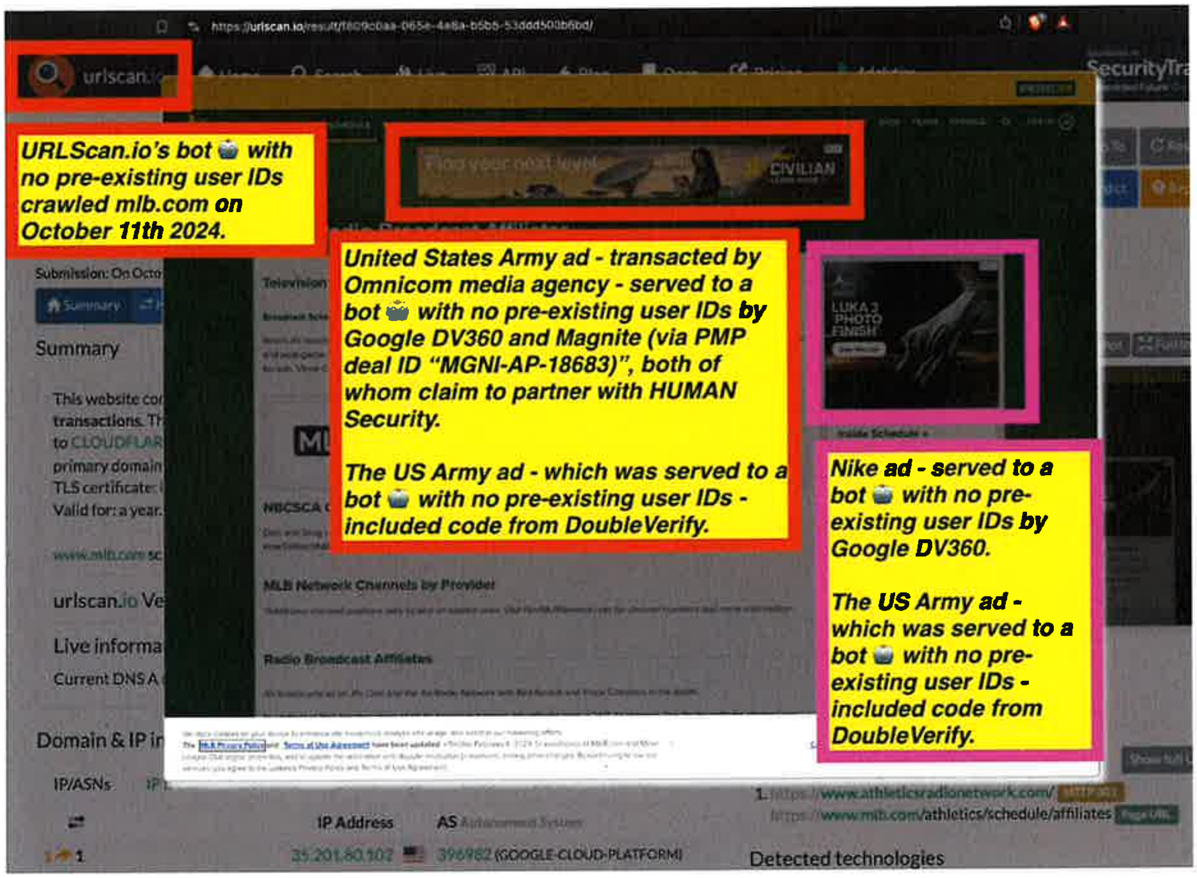
To help further minimize your risk, we have integrated with HUMAN, which serves as an extra safety check for our invalid traffic defenses. This additional safeguard requires no configuration or changes from you.

Note: These additional safeguards are integrated with Display & Video 360. They don't apply to Campaign Manager 360 when used apart from Display & Video 360.

Source: Google Campaign Manager 360 Help - https://support.google.com/campaignmanager/answer/6076504?hl=en

Many brands were observed as having their ads served to bots with no pre-existing user IDs operating out of data center IP addresses. In many cases, the bots were declared bots whose user agent has been listed on the IAB Tech Lab's Bots & Spiders List since 2013.

For example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website mlb.com on October 11th 2024 with no pre-existing user IDs. While the bot was crawling mlb.com, the bot was served an ad for the United States Army. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify. A Nike shoes ad was also served to the bot by DV360 and contained code from DoubleVerify.


https://urlscan.io/result/f809c0aa-065e-4e8a-b5b5-53ddd500b6bd/
urlscan.io
Submission: On Octo
Summary
Find your next level
CIVILIAN
LUKA 3 PHOTO FINISH
Television
MLB Network Channels by Provider
Radio Broadcast Affiliates
NBCSCA
urlscan.io Ve
Live informa
Current DNS A
Domain & IP in
IP/ASNs
IP Address
AS Autonomous System
35.201.80.102
396982 (GOOGLE-CLOUD-PLATFORM)
https://www.athleticsradionetwork.com/
https://www.mlb.com/athletics/schedule/affiliates
Detected technologies

URLScan.io's bot 🤖 with no pre-existing user IDs crawled mlb.com on October 11th 2024.

United States Army ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 and Magnite (via PMP deal ID "MGNI-AP-18683)", both of whom claim to partner with HUMAN Security.

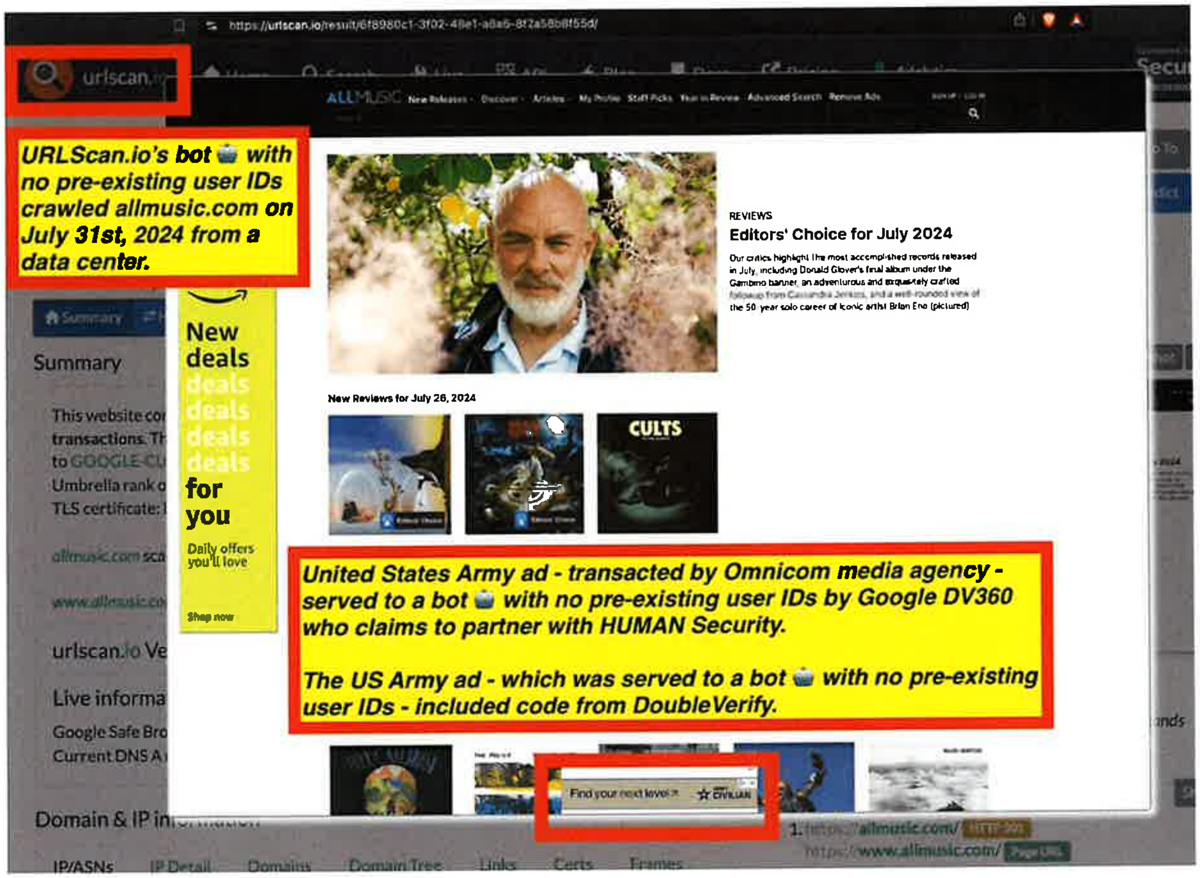
The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Nike ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/f809c0aa-065e-4e8a-b5b5-53ddd500b6bd/#summary

As a second example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website allmusic.com on July 31st, 2024 with no pre-existing user IDs. While the bot was crawling allmusic.com, it served an ad for the United States Army. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.



*URLScan.io's **bot** 🤖 with no pre-existing user IDs crawled allmusic.com **on July 31st**, 2024 from **a data center.***

*United States Army ad - transacted by Omnicom media **agency** - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.*

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

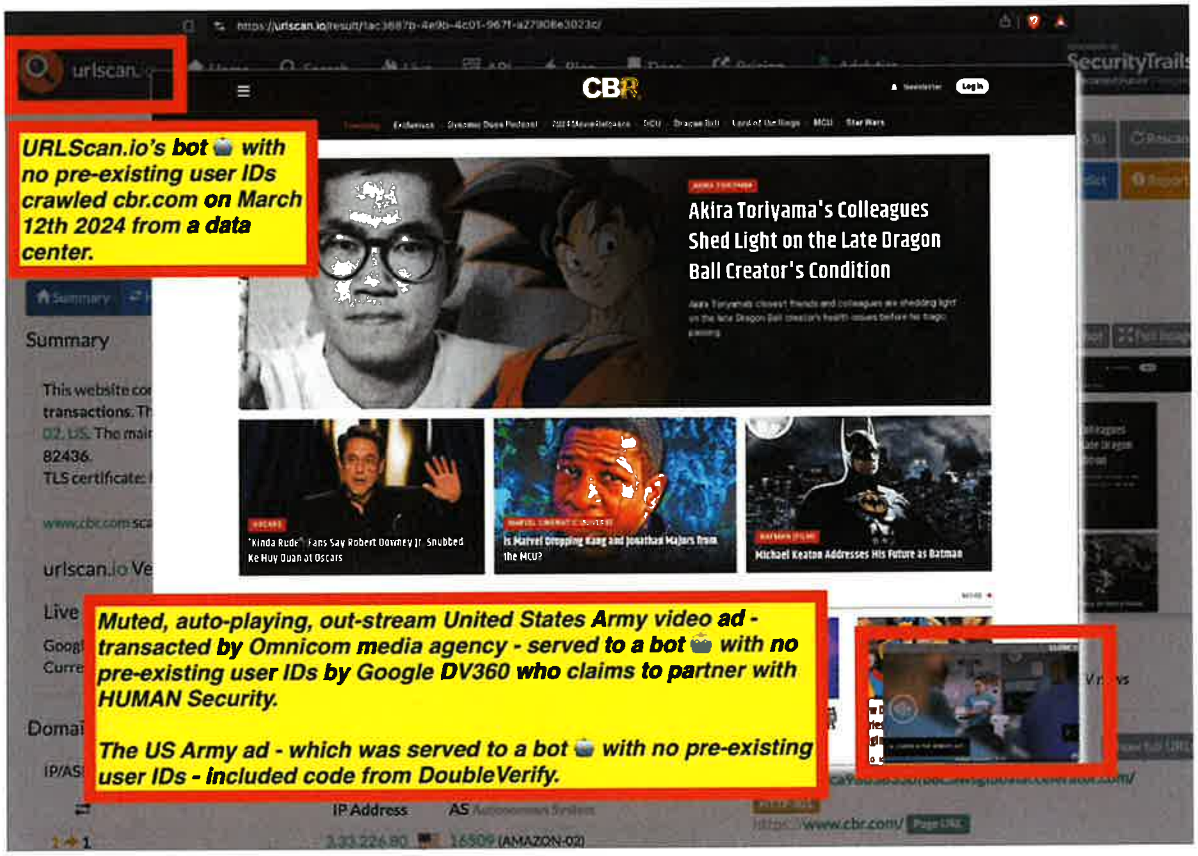
REVIEWS

Editors' Choice for July 2024

Our critics highlight the most accomplished records released in July, including Donald Glover's final album under the Gambino banner, an adventurous and exquisitely crafted followup from Cassandra Jenkins, and a well-rounded view of the 50-year solo career of iconic artist Brian Eno (pictured)

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/6f8980c1-3f02-48e1-a8a6-8f2a58b8f55d/#summary

As a third example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website cbr.com on March 12th 2024 with no pre-existing user IDs. While the bot was crawling cbr.com, it was served an ad for the United States Army. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled cbr.com on March 12th 2024 from a data center.

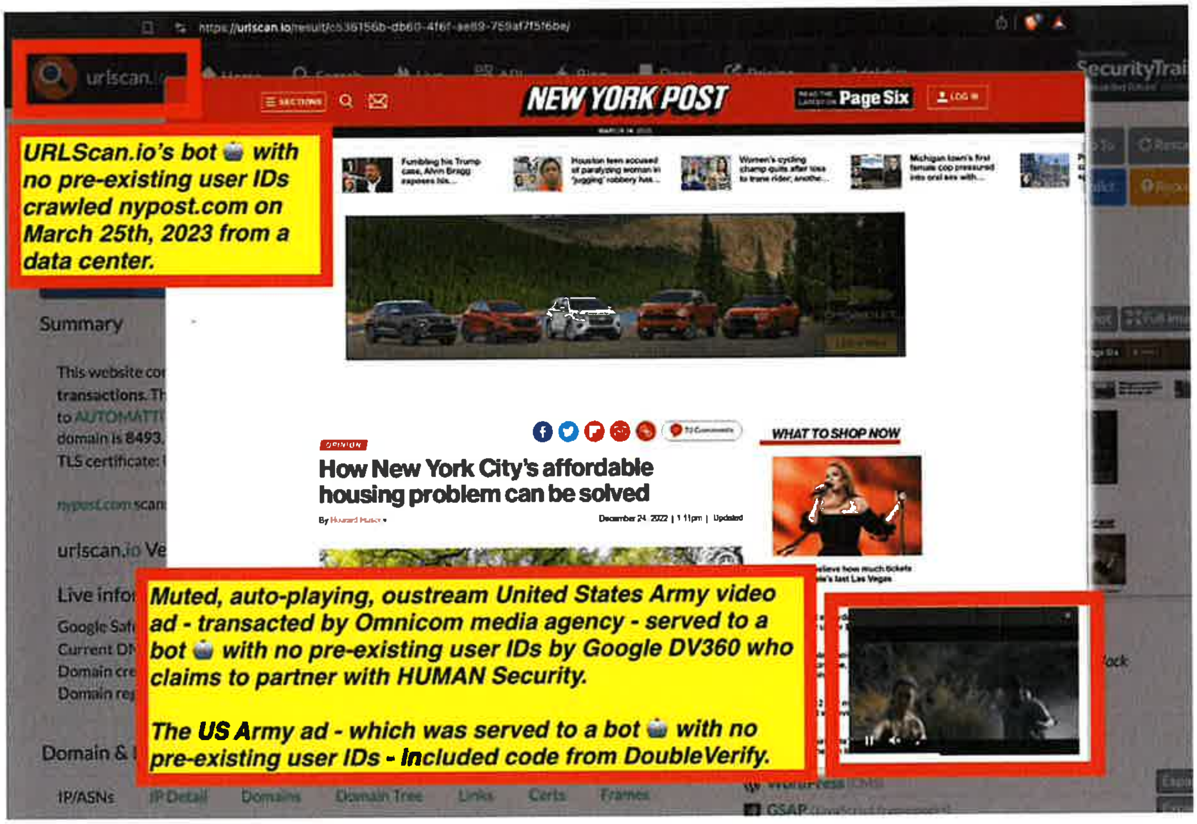
Muted, auto-playing, out-stream United States Army video ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

urlscan.io
CBR
SecurityTrails
Akira Toriyama's Colleagues Shed Light on the Late Dragon Ball Creator's Condition
"Kinda Rude" Fans Say Robert Downey Jr. Snubbed Ke Huy Quan at Oscars
Is Marvel Dropping Kang and Jonathan Majors from the MCU?
Michael Keaton Addresses His Future as Batman
Summary
urlscan.io Ve
Live
Domai
IP/AS
IP Address
AS
16509 (AMAZON-02)
https://www.cbr.com/

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/1ac3687b-4e9b-4c01-967f-a27908e3023c/#summary

As a fourth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website nypost.com on March 25th 2023 with no pre-existing user IDs. While the bot was crawling nypost.com, it was served an "in-stream" video ad for the United States Army in a muted, auto-playing out-stream video slot. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled nypost.com on March 25th, 2023 from a data center.

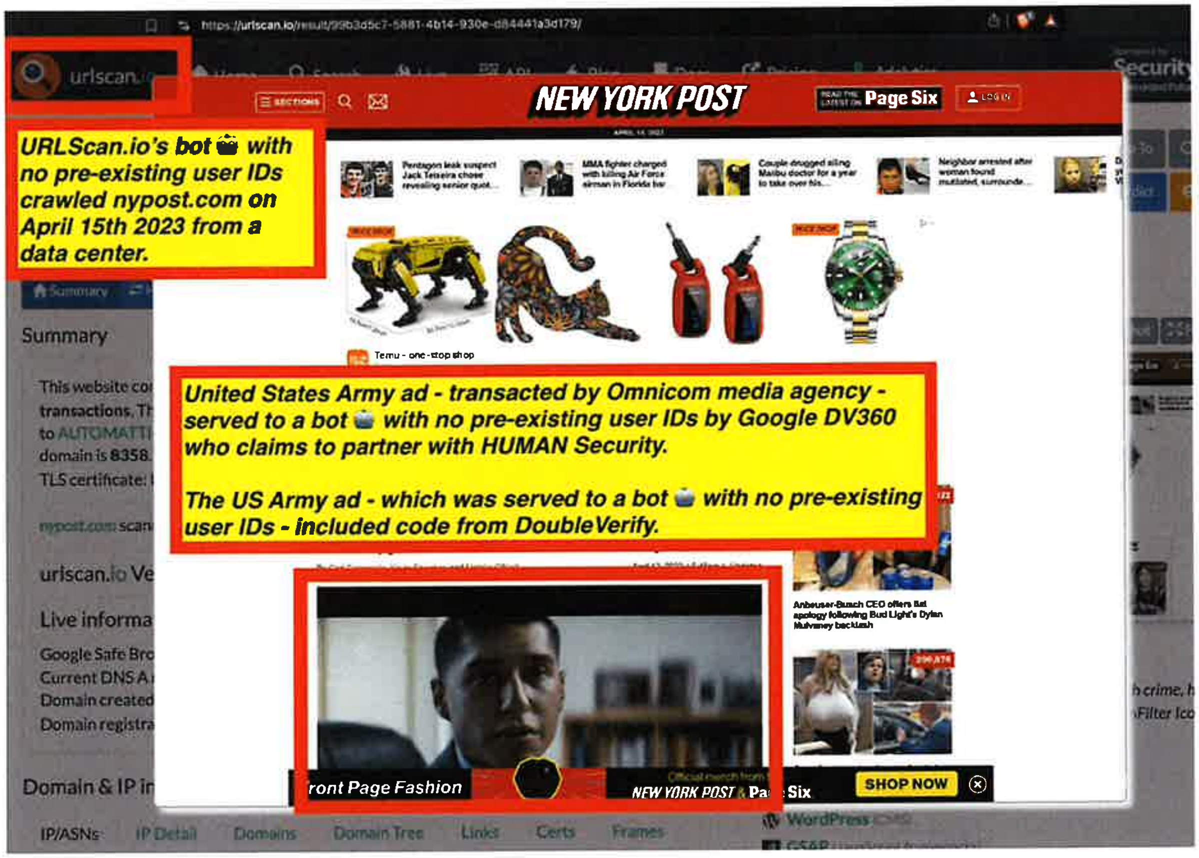
Muted, auto-playing, oustream United States Army video ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - Included code from DoubleVerify.

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/c536156b-db60-4f6f-ae89-759af7f5f6be/

As a fifth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website nypost.com on April 15th 2023 with no pre-existing user IDs. While the bot was crawling nypost.com, it was served an "in-stream" video ad for the United States Army in a muted, auto-playing out-stream video slot. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.

A video ad for the Centers for Disease Control and Prevention vaccine.gov was also served to the bot with no user IDs. The clickthrough URL on the vaccines.gov video ad "vaccines.gov/?s_cid=35527:15_Opening-video:prg.dv:p:RG:GM:A25-49:VC3UV:FY2". The video ad is not visible in the screenshot generated by the bot. The video ad was wrapped in IAS VAST tag wrappers and transacted by Google DV360 DSP and includes references to Reingold media agency.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled nypost.com on April 15th 2023 from a data center.

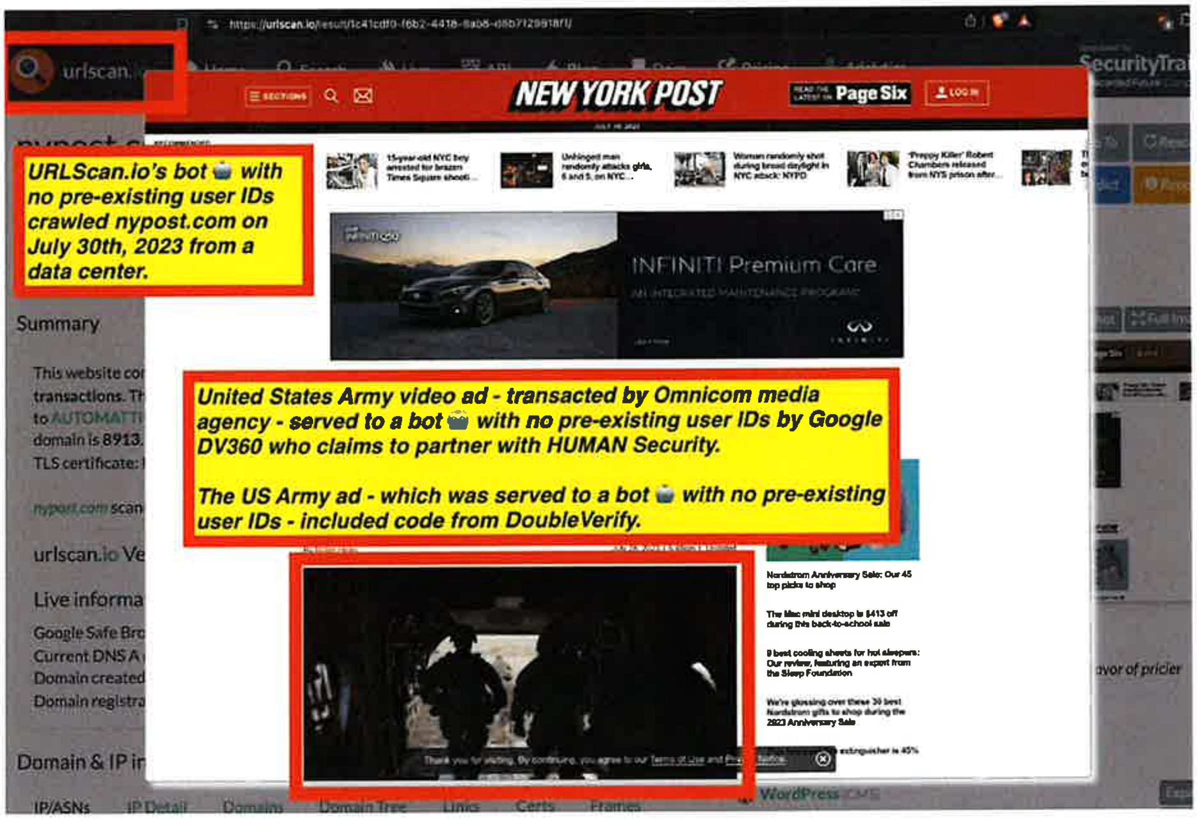
United States Army ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. A vaccines.gov video ad wrapped in IAS tags was also served to the bot, but is not visible in the screenshot.The Army video ad can be seen in full here Army video ad - https://perma.cc/PVB3-F5V5. Source: https://urlscan.io/result/99b3d5c7-5881-4b14-930e-d84441a3d179/;

As a sixth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website nypost.com on July 30th

2023 with no pre-existing user IDs. While the bot was crawling nypost.com, it was served an "in-stream" video ad for the United States Army in a muted, auto-playing out-stream video slot. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.



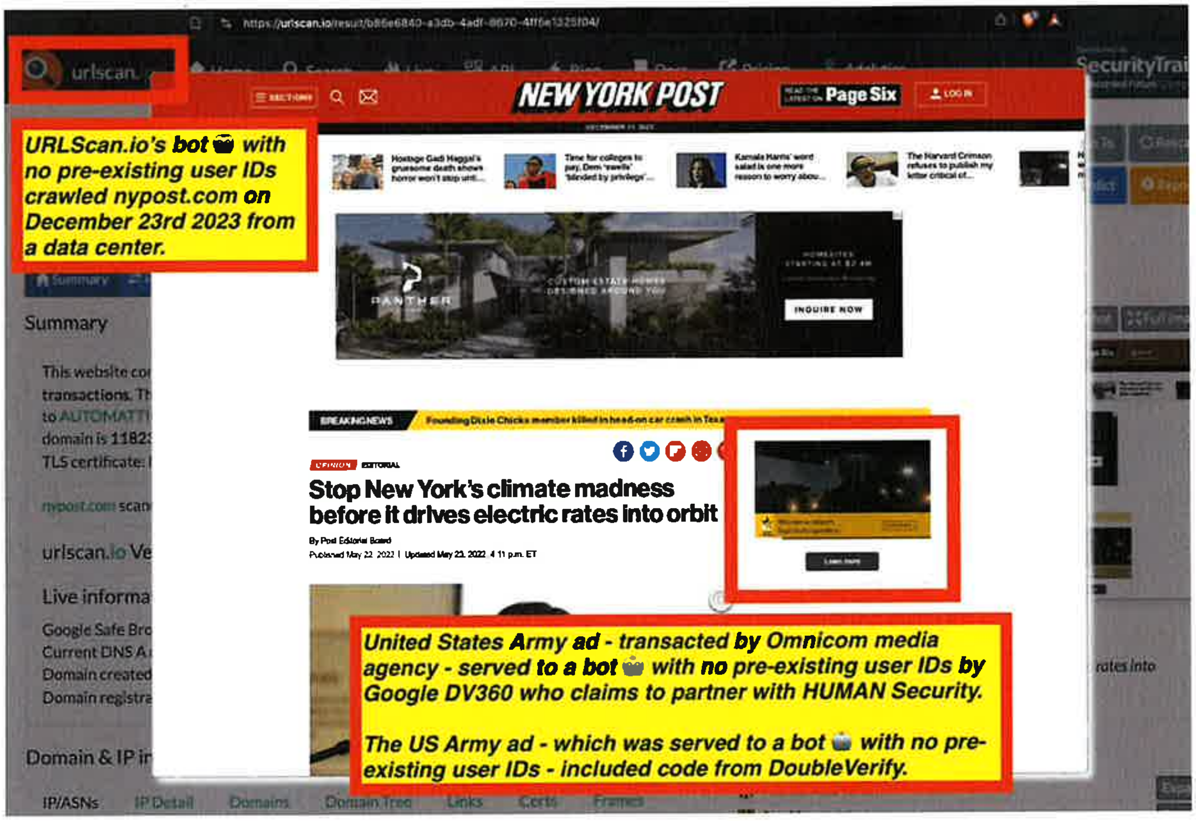
URLScan.io's bot 🤖 with no pre-existing user IDs crawled nypost.com on July 30th, 2023 from a data center.

United States Army video ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/1c41cdf0-f6b2-4418-8ab8-d8b7129818f1/#summary

As a seventh example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website nypost.com on December 23rd 2023 with no pre-existing user IDs. While the bot was crawling nypost.com, the bot was served an ad for the United States Army. The source code of the US Army ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the ad suggests that the ad was transacted by Omnicom media agency, and the Army ad includes code from verification vendor DoubleVerify.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled nypost.com on December 23rd 2023 from a data center.

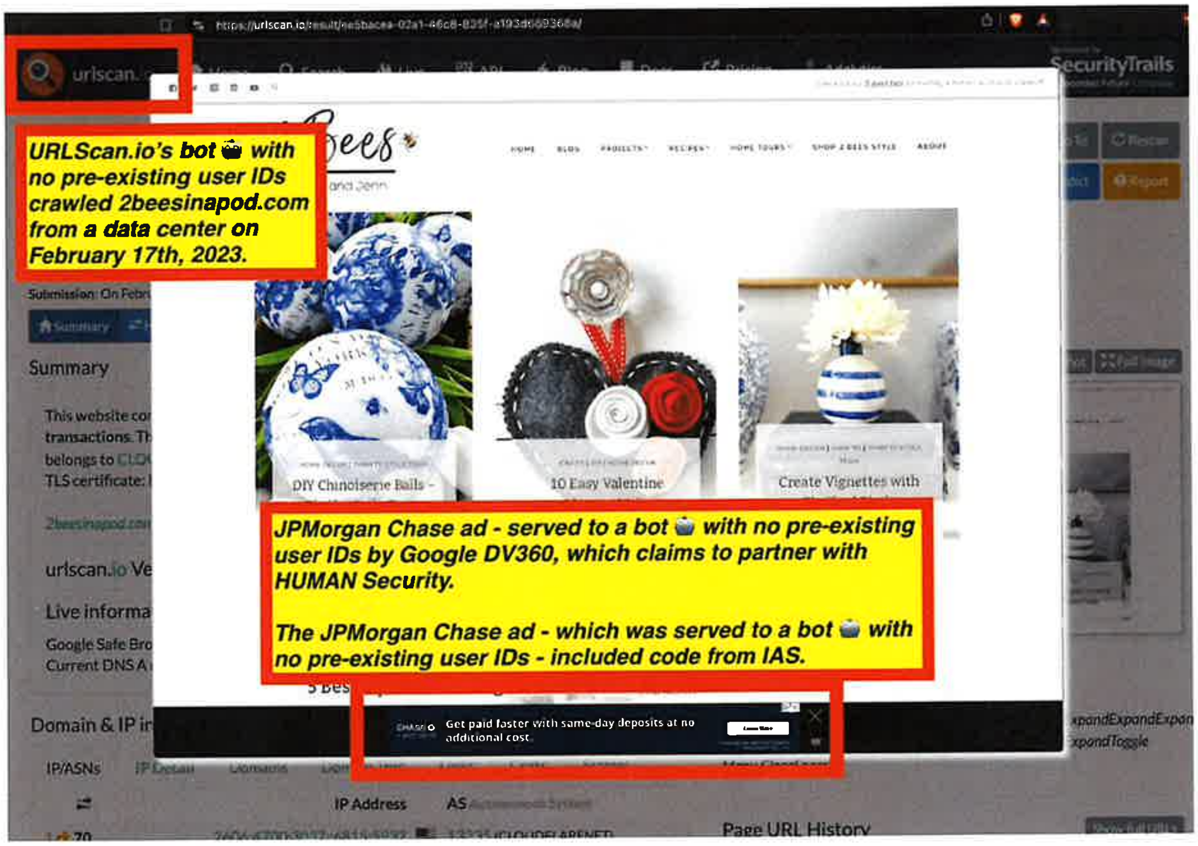
United States Army ad - transacted by Omnicom media agency - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The US Army ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Stop New York's climate madness before it drives electric rates into orbit

Screenshot of a US Army ad served to a bot. The US Army ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security) and Omnicom media agency. The Army ad includes code from DoubleVerify. Source: https://urlscan.io/result/b86e6840-a3db-4adf-8670-4ff5e1325f04/

As an eighth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website 2beesinapod.com on February 17th, 2023 with no pre-existing user IDs. While the bot was crawling 2beesinapod.com, the bot was served an ad for the JPMorgan Chase. The source code of the JPMorgan Chase ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the JPMorgan Chase ad included code from verification vendor IAS.



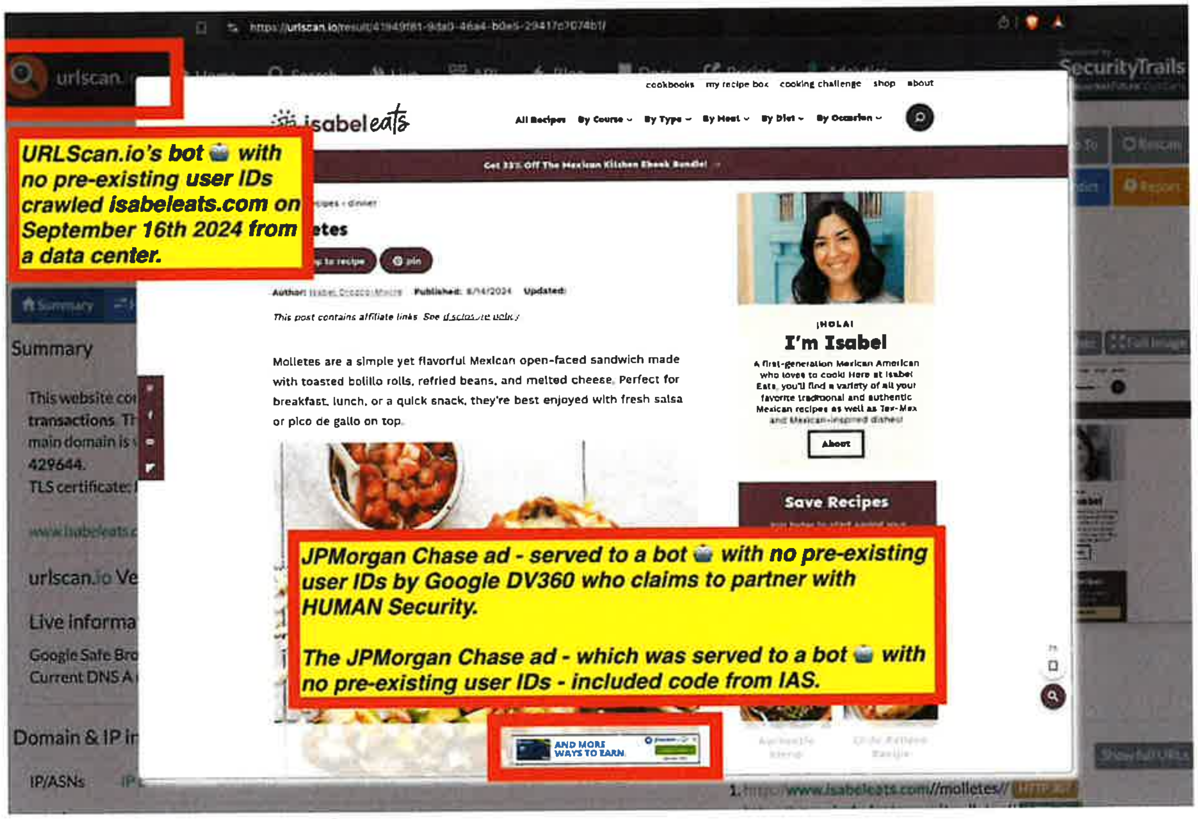
URLScan.io's **bot** 🤖 with no pre-existing user IDs crawled 2beesinapod.com from **a data center** on February 17th, 2023.

JPMorgan Chase ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360, which claims to partner with HUMAN Security.

The JPMorgan Chase ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from IAS.

Screenshot of a JPMorgan Chase ad served to a bot. The JPMorgan Chase appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The JPMorgan Chase ad includes code from IAS. Source: https://urlscan.io/result/ee5bacea-02a1-46c8-835f-a193d669368a/#summary

As a ninth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website isabeleats.com on September 16th, 2024 with no pre-existing user IDs. While the bot was crawling isabeleats.com, the bot was served an ad for the JPMorgan Chase. The source code of the JPMorgan Chase ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the JPMorgan Chase ad included code from verification vendor IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled isabeleats.com on September 16th 2024 from a data center.

JPMorgan Chase ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The JPMorgan Chase ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from IAS.

This post contains affiliate links. See disclosure policy

Molletes are a simple yet flavorful Mexican open-faced sandwich made with toasted bolillo rolls, refried beans, and melted cheese. Perfect for breakfast, lunch, or a quick snack, they're best enjoyed with fresh salsa or pico de gallo on top.

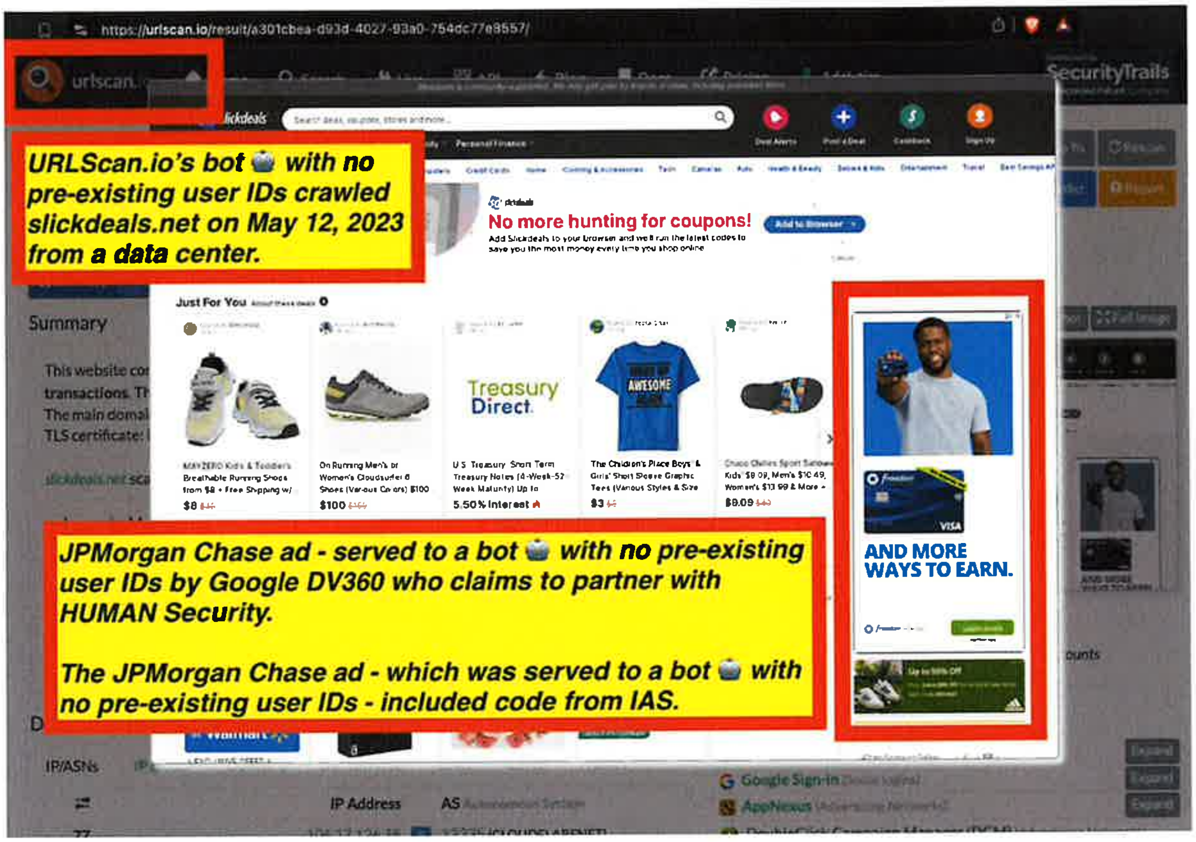
¡HOLA!

I'm Isabel

A first-generation Mexican American who loves to cook! Here at Isabel Eats, you'll find a variety of all your favorite traditional and authentic Mexican recipes as well as Tex-Mex and Mexican-inspired dishes!

Screenshot of a JPMorgan Chase ad served to a bot. The JPMorgan Chase appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The JPMorgan Chase ad includes code from IAS. Source: https://urlscan.io/result/41949f81-9da0-46a4-b0e5-29417c7074b1/

As a tenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website slickdeals.net on May 12th 2023 with no pre-existing user IDs. While the bot was crawling slickdeals.net, the bot was served an ad for the JPMorgan Chase. The source code of the JPMorgan Chase ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the JPMorgan Chase ad included code from verification vendor IAS.



https://urlscan.io/result/a301cbea-d93d-4027-93a0-754dc77e8557/

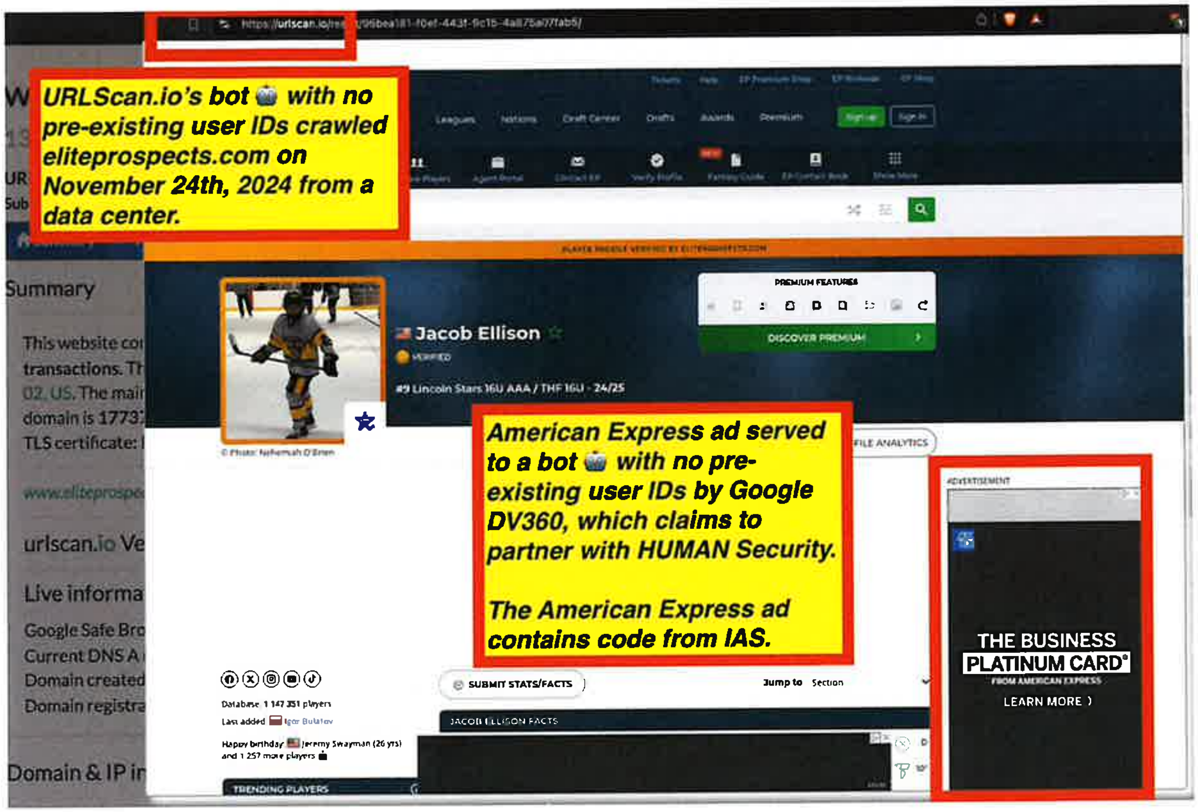
URLScan.io's bot 🤖 with no pre-existing user IDs crawled slickdeals.net on May 12, 2023 from a data center.

JPMorgan Chase ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

The JPMorgan Chase ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from IAS.

Screenshot of a JPMorgan Chase ad served to a bot. The JPMorgan Chase appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The JPMorgan Chase ad includes code from IAS. Source: https://urlscan.io/result/fc75dda4-f6a3-43df-a0c4-c0f969fdfbcc/#summary

As an eleventh example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website eliteprospects.com on November 24th, 2023 with no pre-existing user IDs. While the bot was crawling eliteprospects.com, the bot was served an ad for the American Express. The source code of the American Express ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the American Express ad included code from verification vendor IAS.



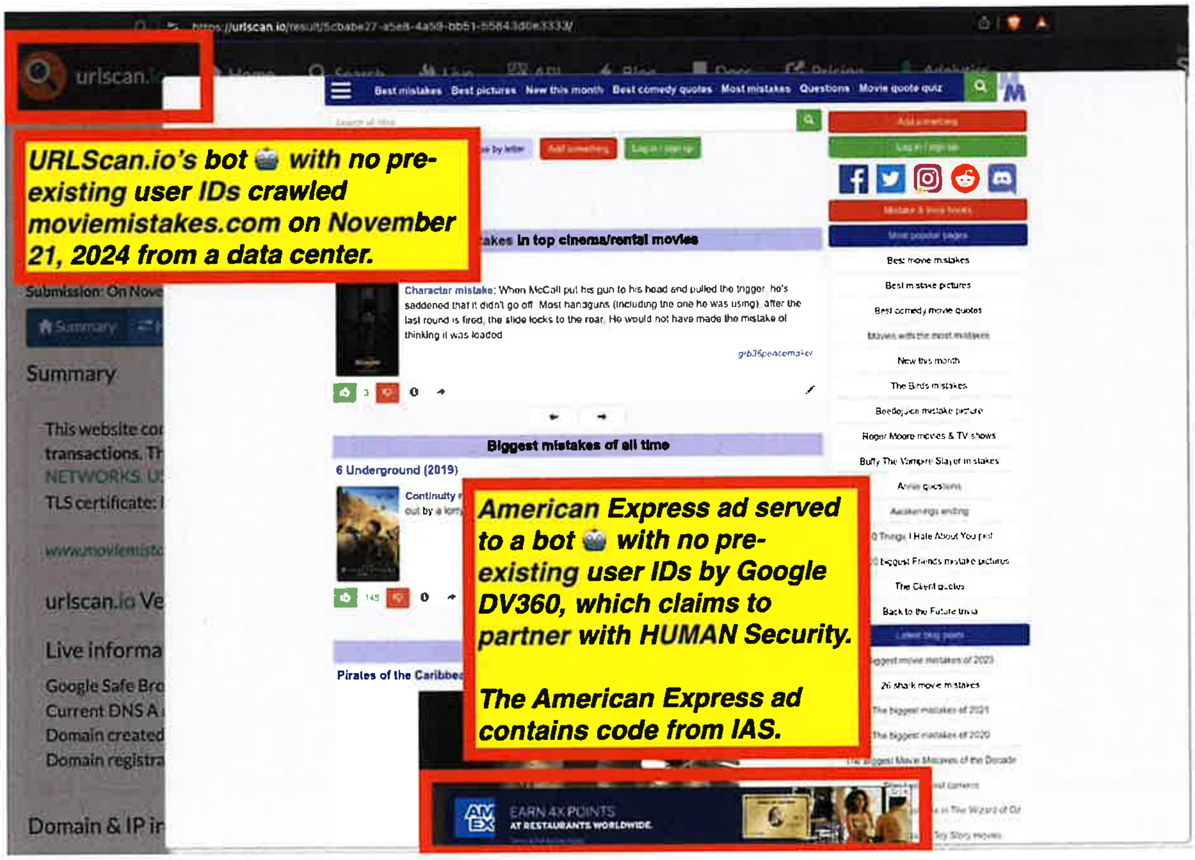
URLScan.io's bot 🤖 with no pre-existing user IDs crawled eliteprospects.com on November 24th, 2024 from a data center.

American Express ad served to a bot 🤖 with no pre-existing user IDs by Google DV360, which claims to partner with HUMAN Security.

The American Express ad contains code from IAS.

Screenshot of an American Express ad served to a bot. The American Express ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The American Express ad includes code from IAS. Source: https://urlscan.io/result/96bea181-f0ef-443f-9c15-4a875a07fab5

As a twelfth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website moviemistakes.com on November 21st, 2024 with no pre-existing user IDs. While the bot was crawling moviemistakes.com, the bot was served an ad for the American Express. The source code of the American Express ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the American Express ad included code from verification vendor IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled moviemistakes.com on November 21, 2024 from a data center.

akes in top cinema/rental movies

Character mistake: When McCall put his gun to his head and pulled the trigger, he's saddened that it didn't go off. Most handguns (including the one he was using), after the last round is fired, the slide locks to the rear. He would not have made the mistake of thinking it was loaded.

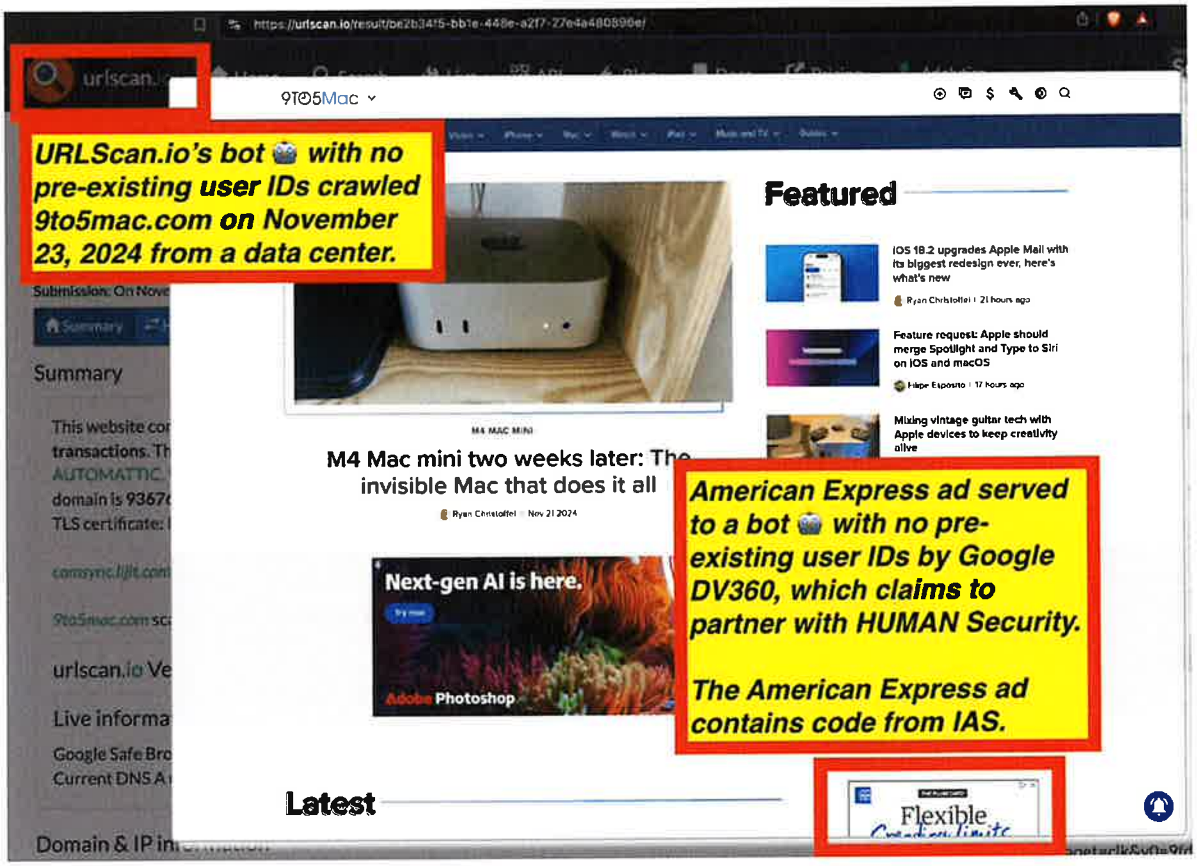
grb36peacemaker

American Express ad served to a bot 🤖 with no pre-existing user IDs by Google DV360, which claims to partner with HUMAN Security.

The American Express ad contains code from IAS.

Screenshot of an American Express ad served to a bot. The American Express ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The American Express ad includes code from IAS. Source: https://urlscan.io/result/5cbabe27-a5e8-4a59-bb51-55843d0e3333/

As a thirteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website 9to5mac.com on November 23, 2024 with no pre-existing user IDs. While the bot was crawling 9to5mac.com, the bot was served an ad for the American Express. The source code of the American Express ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the American Express ad included code from verification vendor IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled 9to5mac.com on November 23, 2024 from a data center.

iOS 18.2 upgrades Apple Mail with its biggest redesign ever, here's what's new

Feature request: Apple should merge Spotlight and Type to Siri on iOS and macOS

Mixing vintage guitar tech with Apple devices to keep creativity alive

M4 MAC MINI

M4 Mac mini two weeks later: The invisible Mac that does it all

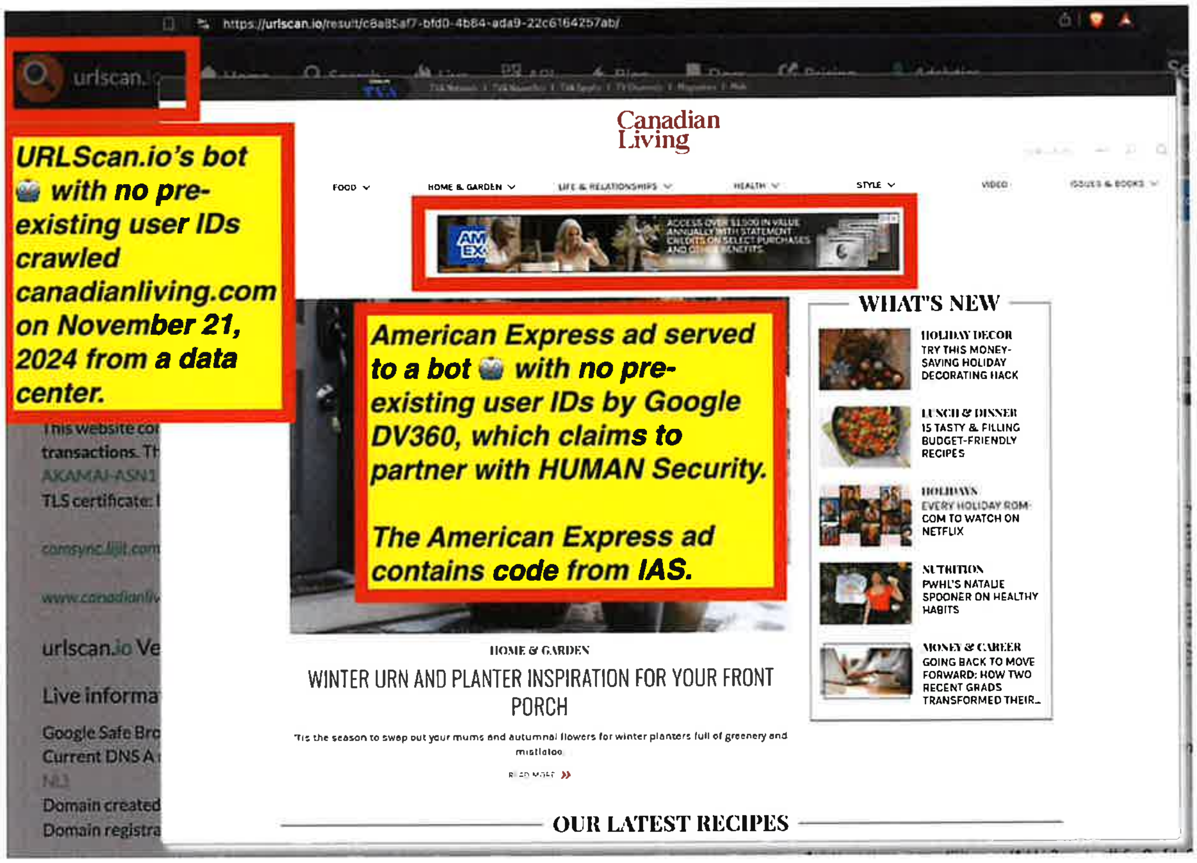
Next-gen AI is here. Adobe Photoshop

American Express ad served to a bot 🤖 with no pre-existing user IDs by Google DV360, which claims to partner with HUMAN Security.

The American Express ad contains code from IAS.

Screenshot of an American Express ad served to a bot. The American Express ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The American Express ad includes code from IAS. Source: https://urlscan.io/result/be2b34f5-bb1e-448e-a2f7-27e4a480896e/

As a fourteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website canadianliving.com on November 21st, 2024 with no pre-existing user IDs. While the bot was crawling canadianliving.com, the bot was served an ad for the American Express. The source code of the American Express ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the American Express ad included code from verification vendor IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled canadianliving.com on November 21, 2024 from a data center.

American Express ad served to a bot 🤖 with no pre-existing user IDs by Google DV360, which claims to partner with HUMAN Security.

The American Express ad contains code from IAS.

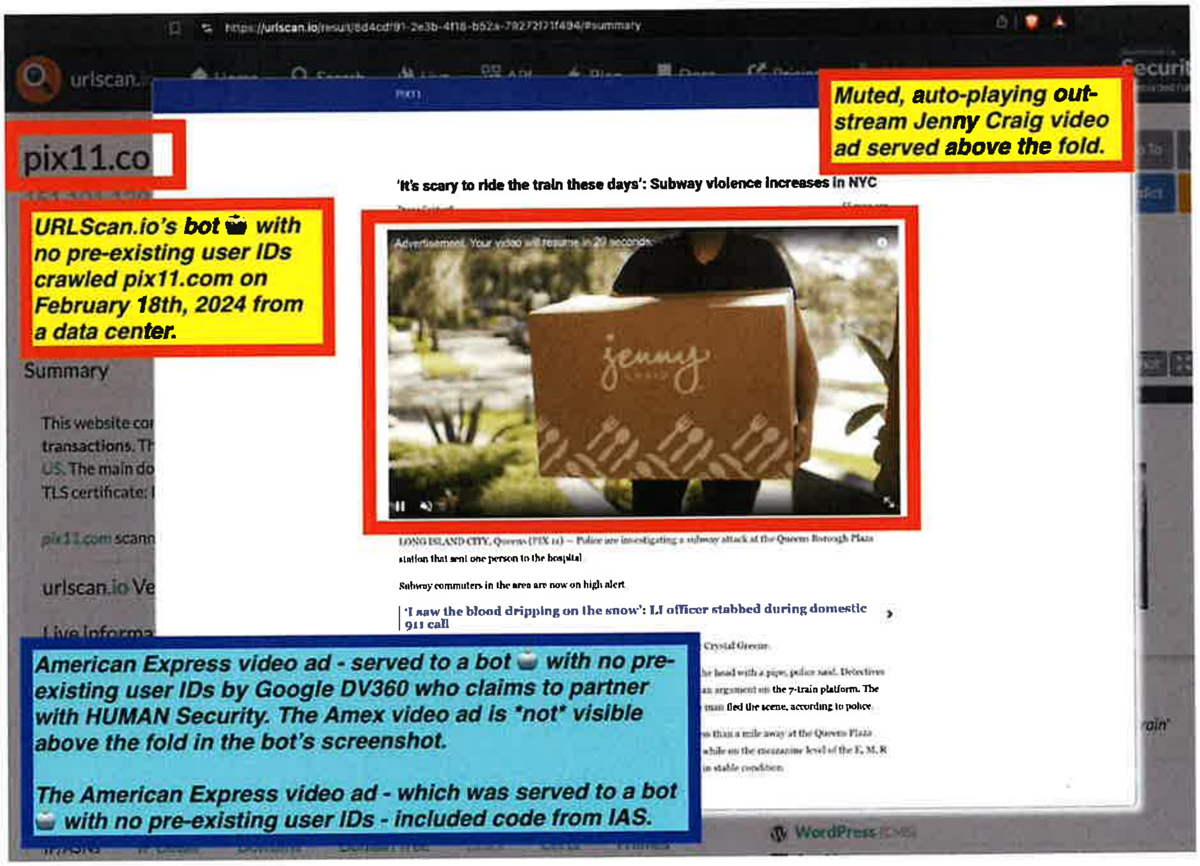
https://urlscan.io/result/c8a85af7-bfd0-4b84-ada9-22c6164257ab/
urlscan.io
Canadian Living
FOOD
HOME & GARDEN
LIFE & RELATIONSHIPS
HEALTH
STYLE
VIDEO
ISSUES & BOOKS
AM EX
ACCESS OVER $1,500 IN VALUE ANNUALLY WITH STATEMENT CREDITS ON SELECT PURCHASES AND OTHER BENEFITS
WHAT'S NEW
HOLIDAY DECOR
TRY THIS MONEY-SAVING HOLIDAY DECORATING HACK
LUNCH & DINNER
15 TASTY & FILLING BUDGET-FRIENDLY RECIPES
HOLIDAYS
EVERY HOLIDAY ROM-COM TO WATCH ON NETFLIX
NUTRITION
PWHL'S NATALIE SPOONER ON HEALTHY HABITS
MONEY & CAREER
GOING BACK TO MOVE FORWARD: HOW TWO RECENT GRADS TRANSFORMED THEIR...
HOME & GARDEN
WINTER URN AND PLANTER INSPIRATION FOR YOUR FRONT PORCH
'Tis the season to swap out your mums and autumnal flowers for winter planters full of greenery and mistletoe.
READ MORE »
OUR LATEST RECIPES
This website co
transactions. Th
AKAMAI-ASN1
TLS certificate: I
comsync.lijit.com
www.canadianliv
urlscan.io Ve
Live informa
Google Safe Bro
Current DNS A
NL
Domain created
Domain registra

Screenshot of an American Express ad served to a bot. The American Express ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The American Express ad includes code from IAS. Source: https://urlscan.io/result/c8a85af7-bfd0-4b84-ada9-22c6164257ab/

As a fifteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website pix11.com on February 18th, 2024 with no pre-existing user IDs. While the bot was crawling February 18th, 2024, the bot was served an "in-stream video" ad for American Express in a muted, out-stream video player. The American Express video ad is not visible above-the-fold in the screenshot generated by URLScan.io's bot.

The source code of the American Express ad shows that the video ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security. The source code of the American Express ad included code from verification vendor IAS.

A muted, auto-playing Jenny Craig (jennycraig.com) video is visible above the fold in the screenshot taken by the bot.


https://urlscan.io/result/8d4cdf91-2e3b-4f18-b52a-79272f71f494/#summary
urlscan.io
pix11.co
Summary
Advertisement: Your video will resume in 29 seconds
WordPress (CMS)

Muted, auto-playing out-stream Jenny Craig video ad served above the fold.

URLScan.io's bot 🤖 with no pre-existing user IDs crawled pix11.com on February 18th, 2024 from a data center.

'It's scary to ride the train these days': Subway violence increases in NYC

LONG ISLAND CITY, Queens (PIX 11) — Police are investigating a subway attack at the Queens Borough Plaza station that sent one person to the hospital.

Subway commuters in the area are now on high alert.

'I saw the blood dripping on the snow': LI officer stabbed during domestic 911 call

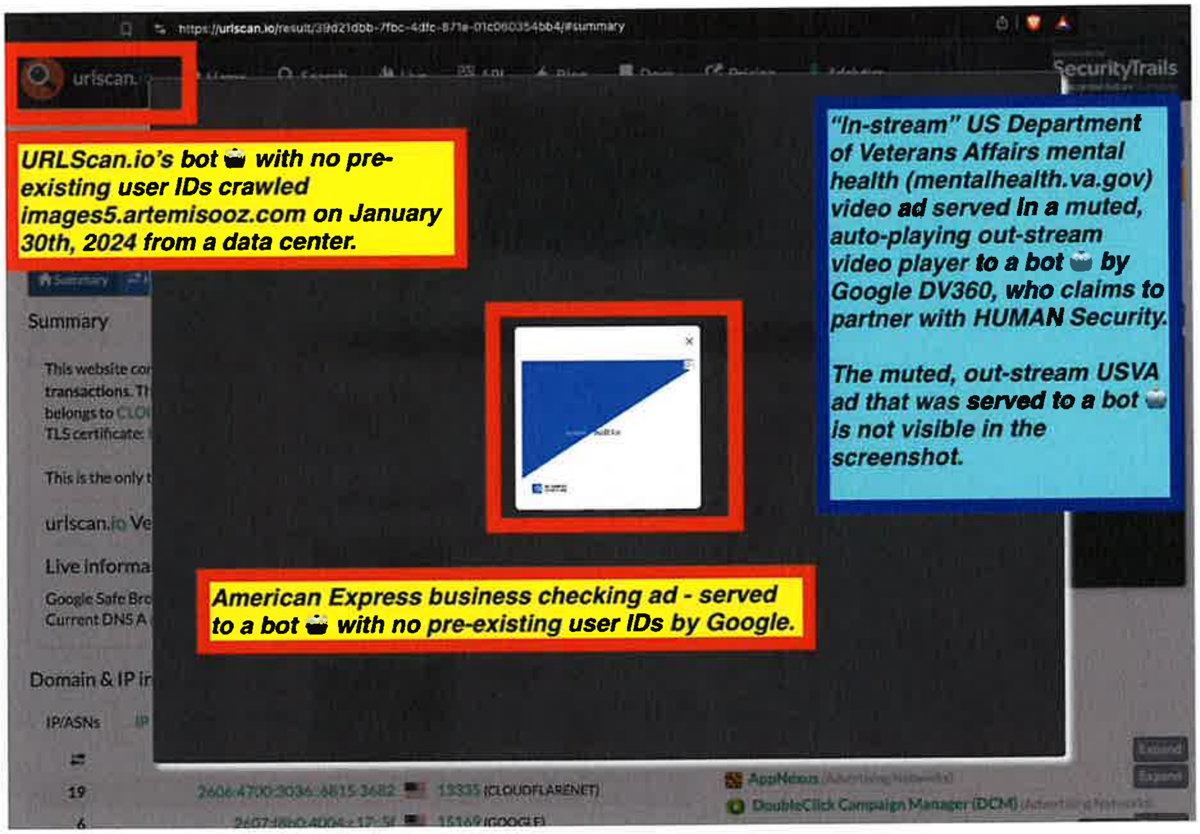
American Express video ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security. The Amex video ad is *not* visible above the fold in the bot's screenshot.

The American Express video ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from IAS.

Screenshot of a Jenny Craig video ad served to a bot. An American Express ad was also served to the bot but is not visible above-the-fold in the screenshot generated by the bot. The American Express video ad creative can be viewed here: https://perma.cc/5QDY-TEMH. The American Express ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). The American Express ad includes code from IAS. Source: https://urlscan.io/result/8d4cdf91-2e3b-4f18-b52a-79272f71f494/#summary

As a sixteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website images5.artemisooz.com on January 30th, 2024 with no pre-existing user IDs. While the bot was crawling images5.artemisooz.com, the bot was served an "in-stream video" ad for the US Department of Veterans Affairs mental health program (mentalhealth.va.gov) in a muted, auto-playing outstream video player. The Veterans Affairs video ad is not visible in the screenshot taken by the URLScan.io bot. The source code of the Department of Veterans Affairs ad shows that the ad was served to the bot (which lacks any pre-existing user identifiers) by Google DV360, which claims to partner with HUMAN Security.

An American Express pop-out banner ad can be seen in the middle of the screenshot taken by the bot.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled images5.artemisooz.com on January 30th, 2024 from a data center.

"In-stream" US Department of Veterans Affairs mental health (mentalhealth.va.gov) video ad served in a muted, auto-playing out-stream video player to a bot 🤖 by Google DV360, who claims to partner with HUMAN Security.

The muted, out-stream USVA ad that was served to a bot 🤖 is not visible in the screenshot.

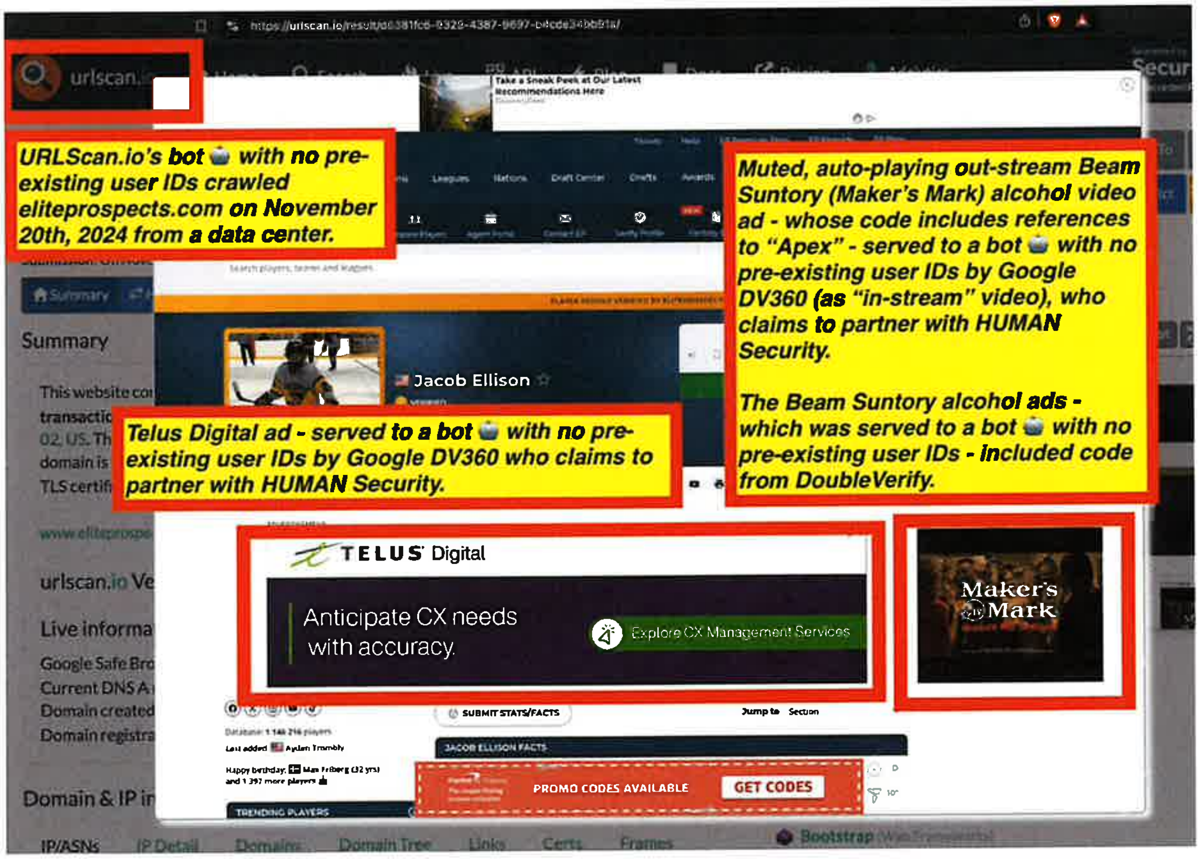
American Express business checking ad - served to a bot 🤖 with no pre-existing user IDs by Google.

Screenshot of an American Express ad that was served to a bot. A US Department of Veterans Affairs (mentalhealth.va.gov) video ad was also served to the bot but is not visible above-the-fold in the screenshot generated by the bot. The Veterans Affairs government video ad creative can be viewed here: https://perma.cc/Z76S-68TZ. The Department of Veterans Affairs ad appears to have been transacted by Google DV360 (which claims to partner with HUMAN Security). Source:

https://urlscan.io/result/39d21dbb-7fbc-4dfc-871e-01c060354bb4/#summary

As a seventeenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website eliteprospects.com on November 20th, 2024 with no pre-existing user IDs. While the bot was crawling eliteprospects.com, the bot was served a "in-stream video" ad for Beam Suntory's Maker's Mark alcohol in muted, auto-playing outstream video player. The source code of the muted outstream Beam Suntory's Maker's Mark video ads that were served to the bot (which lacks any pre-existing user identifiers) show that the ad were served by Google DV360, which claims to partner with HUMAN Security. The Beam Suntory ads also include code from verification vendor DoubleVerify.

A Telus Digital ad was also served by DV360 to the bot.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled eliteprospects.com on November 20th, 2024 from a data center.

Muted, auto-playing out-stream Beam Suntory (Maker's Mark) alcohol video ad - whose code includes references to "Apex" - served to a bot 🤖 with no pre-existing user IDs by Google DV360 (as "in-stream" video), who claims to partner with HUMAN Security.

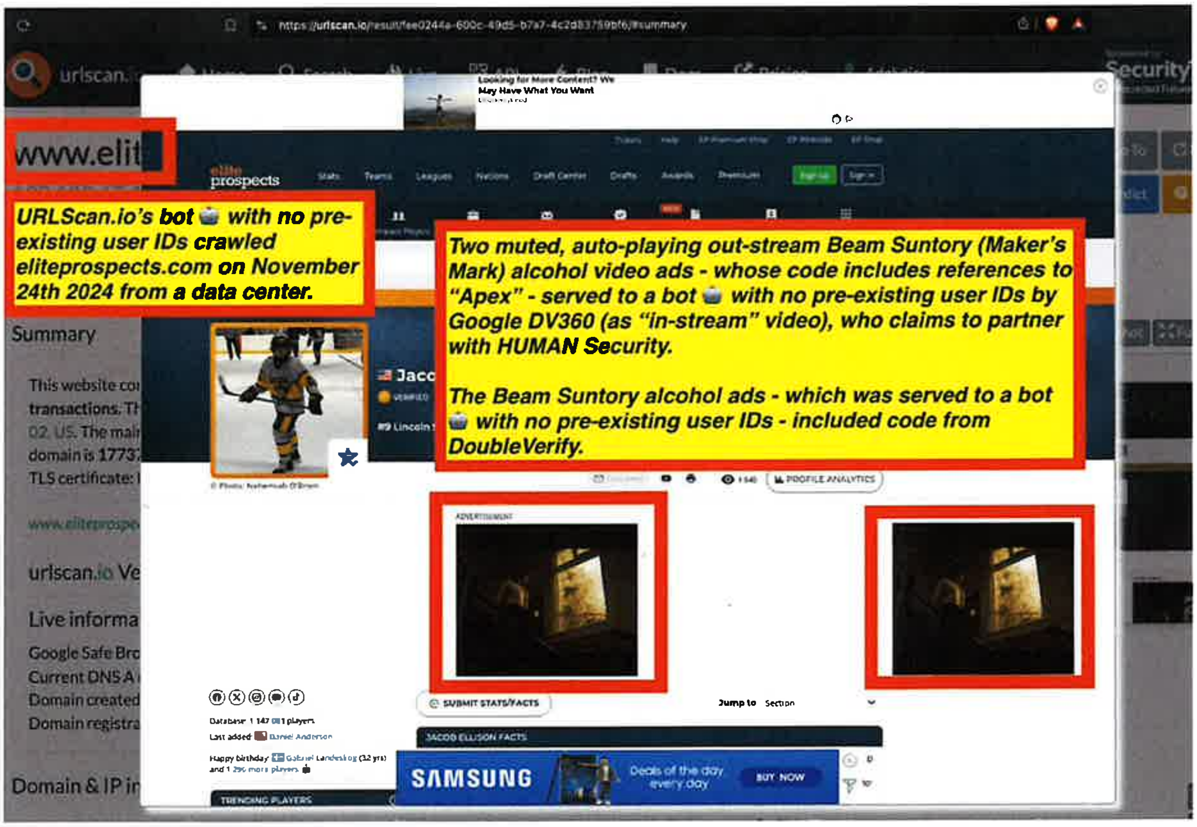
The Beam Suntory alcohol ads - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Telus Digital ad - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

Screenshot of a Beam Suntory Maker's Mark alcohol ad served to a bot. The Beam Suntory ad appears to have been transacted by Google

DV360 (which claims to partner with HUMAN Security). The Beam Suntory ad includes code from DoubleVerify. Source: https://urlscan.io/result/d6381fc6-9329-4387-9697-b4cde34bb91a/#summary

As an eighteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website eliteprospects.com on November 24th, 2024 with no pre-existing user IDs. While the bot was crawling eliteprospects.com, the bot was served two "in-stream video" ads for Beam Suntory's Maker's Mark alcohol in muted, auto-playing outstream video players. The source code of the muted outstream Beam Suntory's Maker's Mark video ads that were served to the bot (which lacks any pre-existing user identifiers) show that the ads were served by Google DV360, which claims to partner with HUMAN Security. The Beam Suntory ads also include code from verification vendor DoubleVerify. A Samsung ad was also served to the bot.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled eliteprospects.com on November 24th 2024 from a data center.

Two muted, auto-playing out-stream Beam Suntory (Maker's Mark) alcohol video ads - whose code includes references to "Apex" - served to a bot 🤖 with no pre-existing user IDs by Google DV360 (as "in-stream" video), who claims to partner with HUMAN Security.

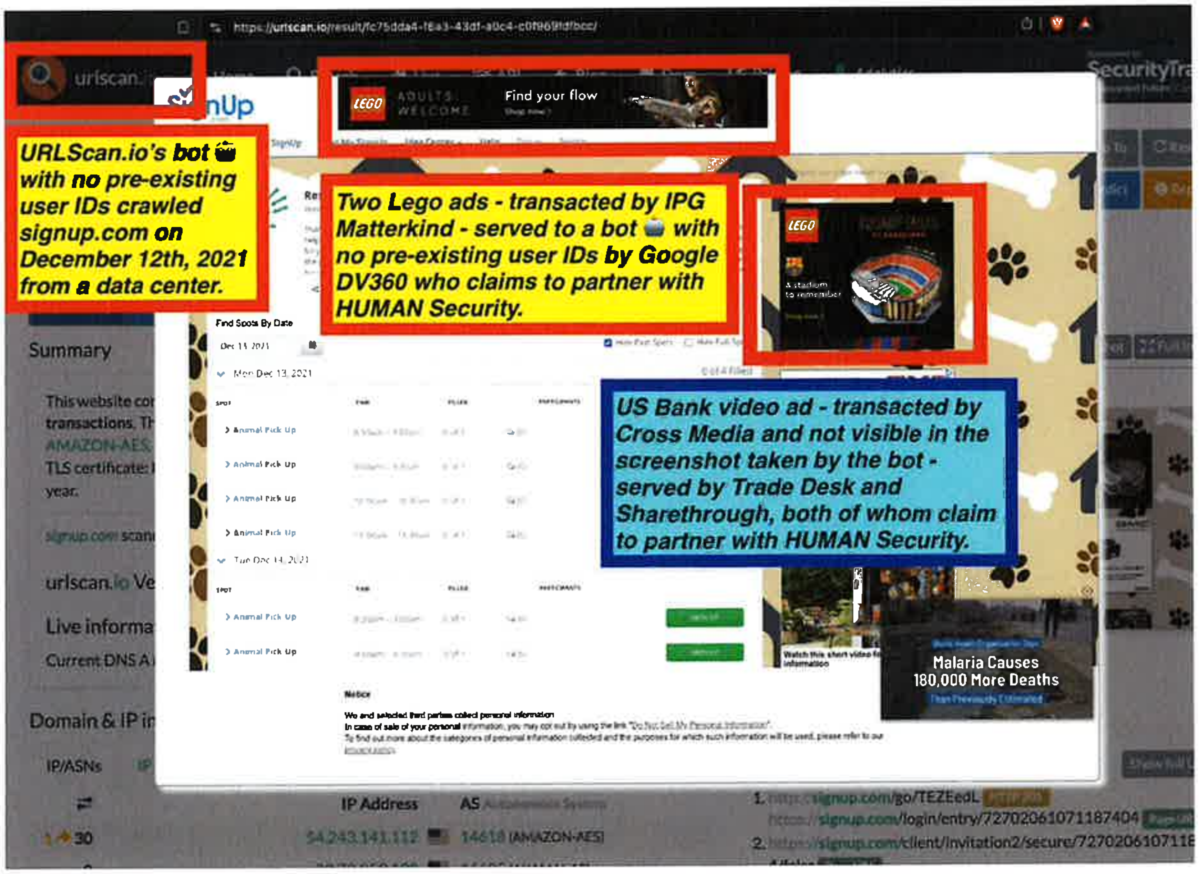
The Beam Suntory alcohol ads - which was served to a bot 🤖 with no pre-existing user IDs - included code from DoubleVerify.

Screenshot of two Beam Suntory Maker's Mark alcohol ads served to a bot. The Beam Suntory ads appears to have been transacted by Google

DV360 (which claims to partner with HUMAN Security). The Beam Suntory ad includes code from DoubleVerify. Source: https://urlscan.io/result/fee0244a-600c-49d5-b7a7-4c2d83759bf6/#summary

As a nineteenth example, in the screenshot below, one can see an instance where URLScan.io's bot crawled the website signup.com on December 12th, 2021 with no pre-existing user IDs. While the bot was crawling signup.com, the bot was shown two Lego ads that were transacted by IPG Matterkind. The source code of the two Lego ads that were shown to the bot (which lacks any pre-existing user identifiers) show that the ad was transacted by Google DV360, which claims to partner with HUMAN Security.

The bot was also served a US Bank video ad that was transacted by Cross Media, Trade Desk DSP, and Sharethrough SSP. Trade Desk and Sharethrough claim to partner with HUMAN Security. The US Bank video ad is not visible in the screenshot taken by the bot.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled signup.com on December 12th, 2021 from a data center.

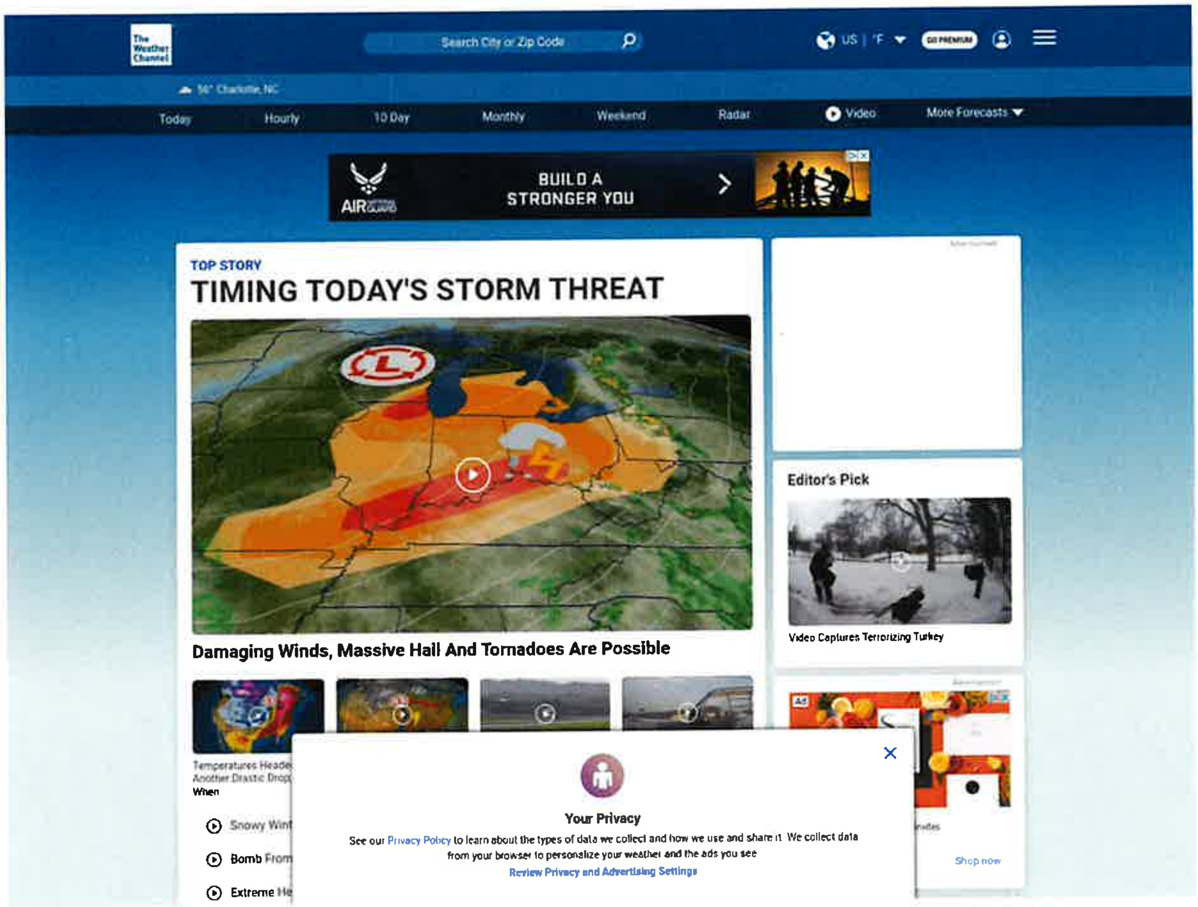
Two Lego ads - transacted by IPG Matterkind - served to a bot 🤖 with no pre-existing user IDs by Google DV360 who claims to partner with HUMAN Security.

US Bank video ad - transacted by Cross Media and not visible in the screenshot taken by the bot - served by Trade Desk and Sharethrough, both of whom claim to partner with HUMAN Security.

https://urlscan.io/result/fc75dda4-f6a3-43df-a0c4-c0f969fdfbce/
urlscan
Find your flow
Summary
Malaria Causes
180,000 More Deaths
IP Address
AS
54.243.141.112
14618 (AMAZON-AES)
https://signup.com/go/TEZEedL
https://signup.com/login/entry/72702061071187404
https://signup.com/client/invitation2/secure/727020610711

Screenshot of two Lego ads served to a bot. The Lego ads appear to have been transacted by Google DV360 (which claims to partner with HUMAN Security). Not visible in the screenshot is a US Bank video ad that was served to the bot by Trade Desk and Sharethrough, both of whom claim to partner with HUMAN Security. Source: https://urlscan.io/result/fc75dda4-f6a3-43df-a0c4-c0f969fdfbcc/

As an additional example, in the screenshot below one can see a US Air Force ad that was transacted by Google Ad Manager (GAM) and DV360 to URLScan.io's bot. The bot was crawling weather.com on February 27th, 2024, when the Air Force ad was served. Weather.com appears to utilize the publisher optimization tools of IAS on its pages, which labeled the bot as "fr=false". The URLScan.io crawl link is: *https://urlscan.io/result/98797fe7-ac9f-4691-bfe4-e6c70c06442c/*



TOP STORY

TIMING TODAY'S STORM THREAT

Damaging Winds, Massive Hail And Tornadoes Are Possible

Temperatures Heade
Another Drastic Drop
When

Snowy Wint

Bomb From

Extreme He

Editor's Pick

Video Captures Terrorizing Turkey

Your Privacy

See our Privacy Policy to learn about the types of data we collect and how we use and share it. We collect data from your browser to personalize your weather and the ads you see

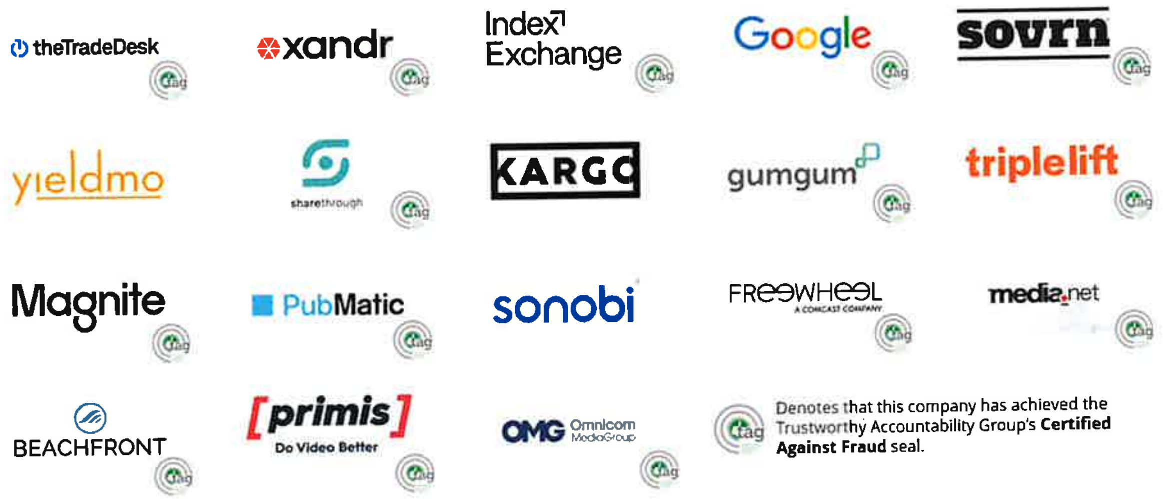
Review Privacy and Advertising Settings

Screenshot showing a US Air Force ad that was served by Google Ad Manager (GAM) and DV360 to URLScan.io's bot whilst the bot was *crawling weather.com on February 27th, 2024. Source: https://urlscan.io/result/98797fe7-ac9f-4691-bfe4-e6c70c06442c/*

Trade Desk and various SSP ads served to bots

Many ad tech vendors who have made public press releases or statements regarding partnering with HUMAN Security (f/k/a White Ops) have been observed serving Fortune 500 and/or US federal government advertises' ads to bots, including declared bots whose user-agents have been on the IAB Tech Labs Bots & Spiders List since 2013. Some of these bots also operate out of various well known data center IP addresses, some of which may potentially be on advertising industry reference lists such as the Trustworthy Accountability Group (TAG's) Data Center IP List.

Ad Tech Vendors & Agencies With Public Partnerships With **Human Security** (f/k/a 'White Ops') Who Transacted Ads to **Declared Bots** (Listed on the IAB Bots & Spiders List Since 2013) Operating From Known Data Center IPs



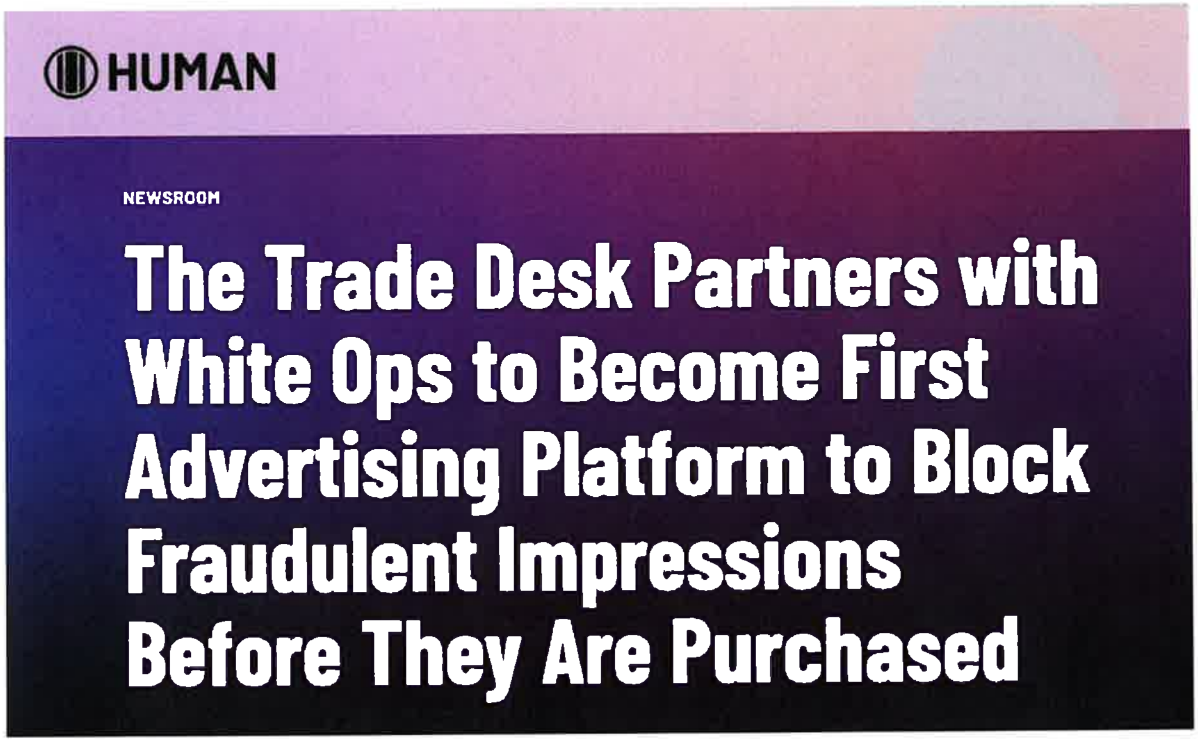
For example, Index Exchange SSP stated in a press release:

"Index Exchange Partners with White Ops to Deliver Invalid Traffic Protection Against Sophisticated Bots Across All Global Inventory Channels"; "Index Exchange (IX), one of the world's largest independent ad exchanges, and White Ops, the global leader in collective protection against sophisticated bot attacks and fraud, today announced an expanded partnership that enhances Index Exchange's global inventory

across all channels and regions. Through White Ops' comprehensive protection, the partnership protects the entirety of Index Exchange's global inventory. It allows buyers to purchase from IX's emerging channels, such as mobile app and Connected TV (CTV), with ***confidence that its supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible****"* (emphasis added).

Demand side platform Trade Desk announced:

"White Ops and The Trade Desk [...] today announce a landmark deal that completely changes how the advertising industry tackles fraud. White Ops' Human Verification technology will aim to ensure that there is a ***human on the other end of every impression served on The Trade Desk*** *that runs through White Ops, in real time, protecting global advertisers and agencies from buying fraudulent impressions [...] For too long, invalid traffic has been part of our industry," said Jeff Green, CEO and co-founder of The Trade Desk. "There's no level of fraud that is acceptable. Our partnership with White Ops means that* ***we are the first advertising platform to block non-human impressions at the front door****. [...] As part of this initiative, White Ops and The Trade Desk will co-locate servers and data centers in North America, Europe and Asia, to* ***scan every biddable ad impression in real-time****. [...] When a non-human impression, known as "Sophisticated Invalid Traffic (SIVT)" within the advertising industry, is identified by White Ops, The Trade Desk will block that impression from serving. The intent is this technology will be* ***applied to every impression*** *The Trade Desk bids on that runs through White Ops, on a global basis. [...] Unlike other solutions, the goal here is to run all impressions across The Trade Desk's platform through White Ops, not just sampled impressions. Additionally, the Trade Desk has collaborated with the leading SSPs to bring a unified solution to market."* (emphasis added).

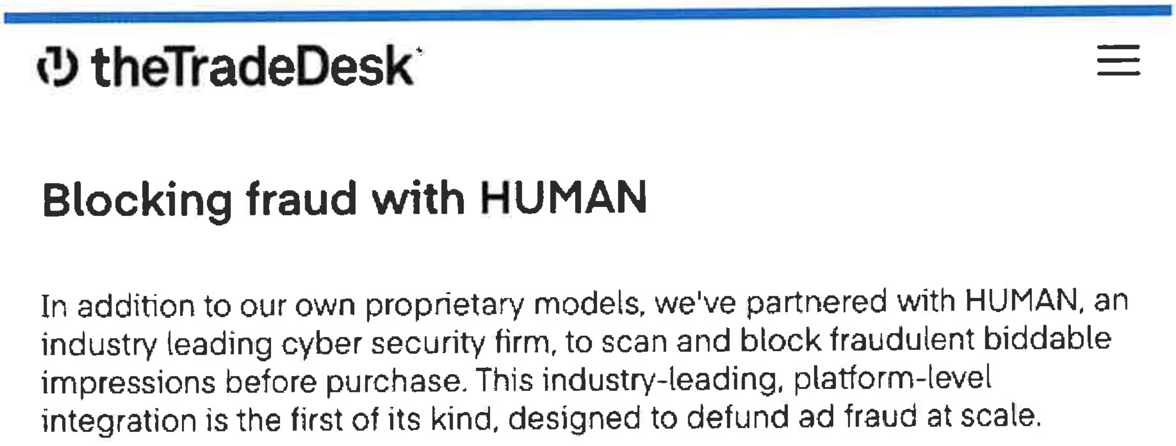


HUMAN

NEWSROOM

The Trade Desk Partners with White Ops to Become First Advertising Platform to Block Fraudulent Impressions Before They Are Purchased

Screenshot of HUMAN Security's website, showing a press release from 2017



theTradeDesk

Blocking fraud with HUMAN

In addition to our own proprietary models, we've partnered with HUMAN, an industry leading cyber security firm, to scan and block fraudulent biddable impressions before purchase. This industry-leading, platform-level integration is the first of its kind, designed to defund ad fraud at scale.

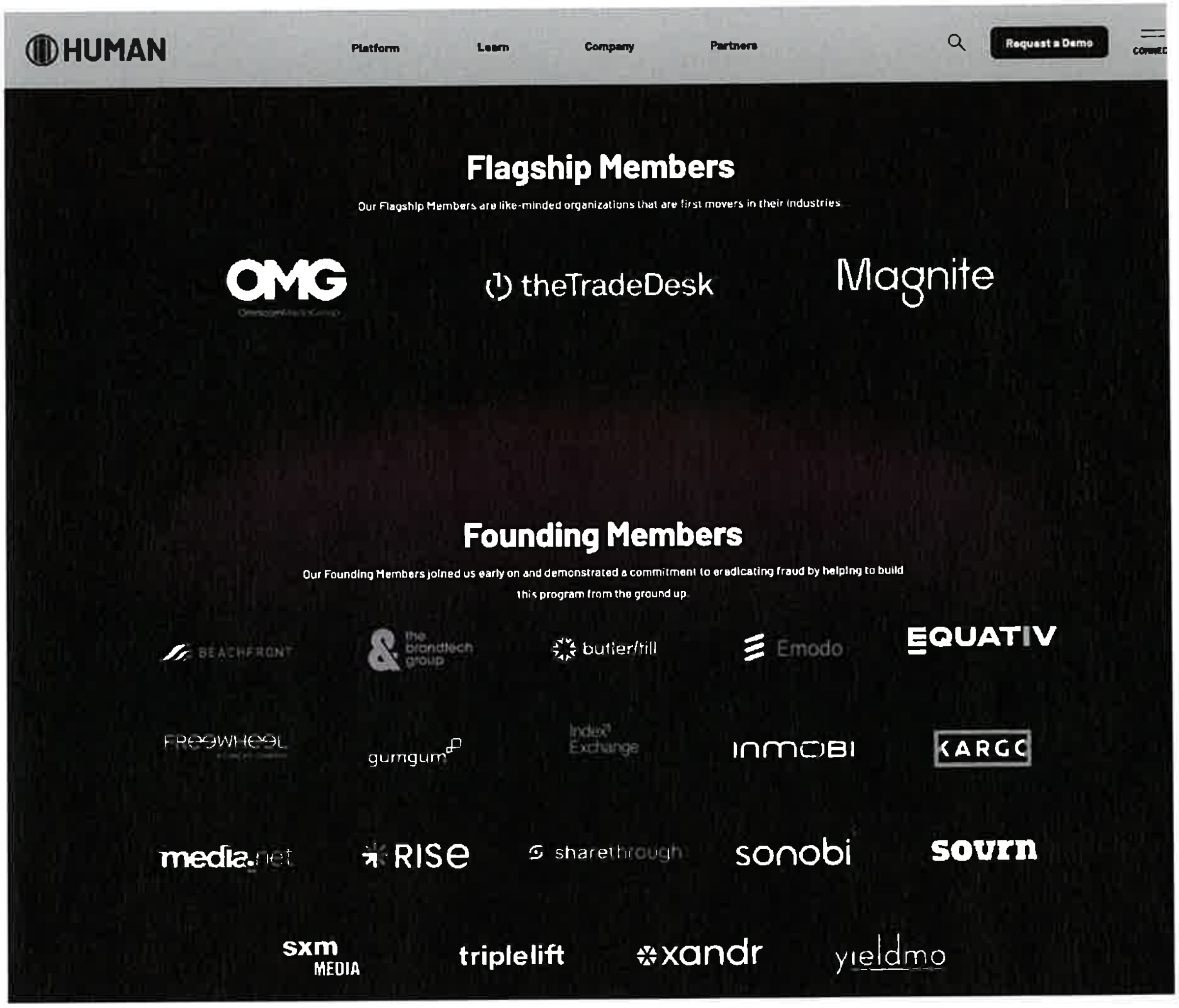
Screenshot of Trade Desk's website, showing the firm partners with HUMAN Securi

Xandr (f/k/a AppNexus) and now owned by Microsoft, announced:

"Xandr [...] and HUMAN, a cybersecurity company best known for collectively protecting enterprises from bot attacks, today announced an

expansion to HUMAN's existing pre-bid bot protection *within the Xandr platform, to provide an additional layer of protection against fraud and sophisticated bot attacks as emerging formats like connected TV (CTV) scale in availability and demand. This integration connects the full breadth of HUMAN's Advertising Integrity suite of ad fraud detection and prevention solutions to Xandr's buy-and sell-side platforms [...] Xandr protects its platform* ***before a bid is even made****—including within CTV—to continue delivering success to its publishers and advertisers. HUMAN recently became the first company to receive accreditation from the Media Rating Council (MRC) for pre and post-bid protection against Sophisticated Invalid Traffic (SIVT) for desktop, mobile web, mobile in-app, and CTV."*

Many ad tech vendors are part of the HUMAN Security's "Human Collective."



Flagship Members

Our Flagship Members are like-minded organizations that are first movers in their industries

Founding Members

Our Founding Members joined us early on and demonstrated a commitment to eradicating fraud by helping to build this program from the ground up

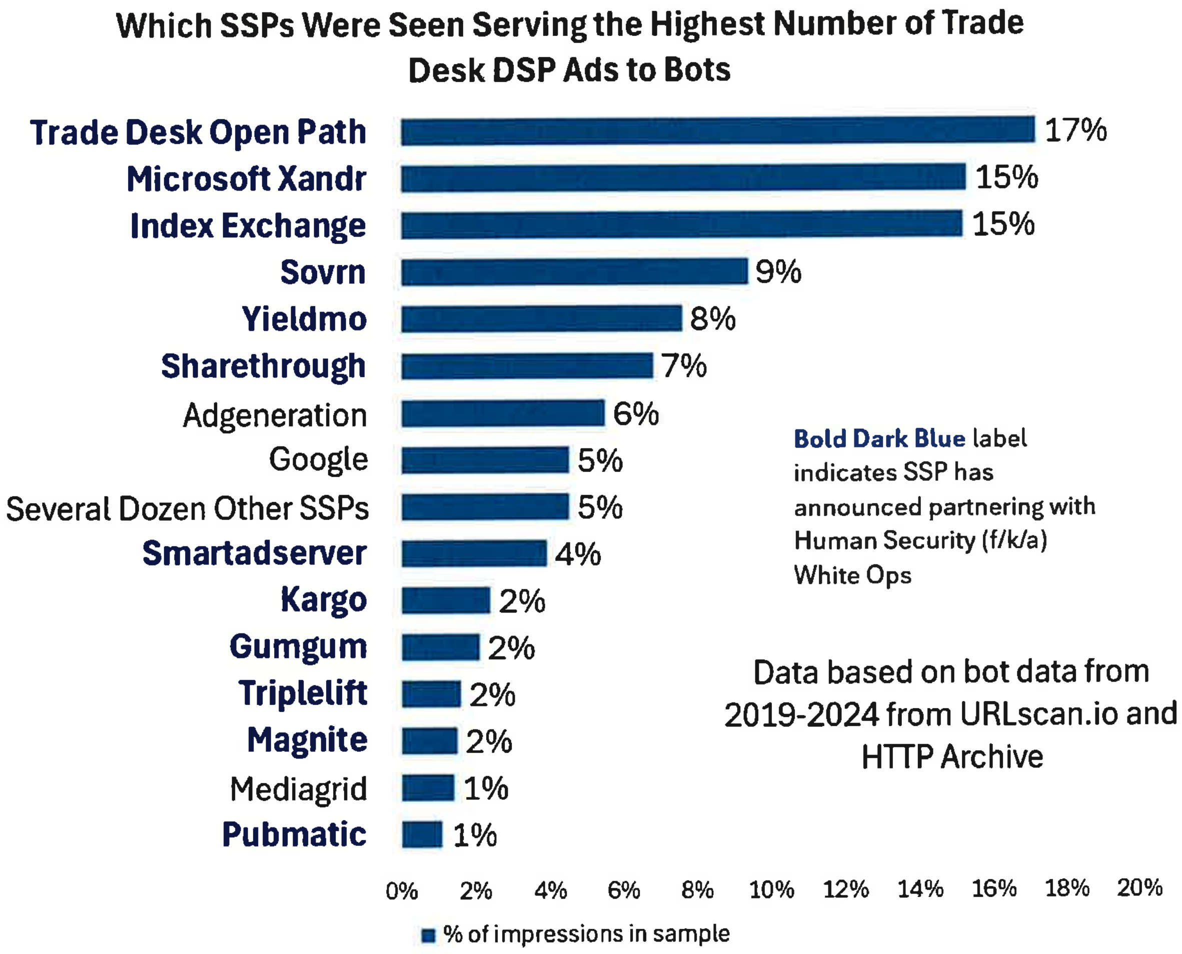
List of Flagship and Founding Members of HUMAN Security's "Human Collective". Source: https://www.humansecurity.com/company/the-human-collective. Participation in the Human Collective entails: "Technology - Powered by HUMAN's proprietary technology and Modern Defense Platform, we can ensure members are protecting themselves and each other."

A list of vendors who issued public statements or claimed to have partnered with HUMAN Security (f/k/a "White Ops") can be seen below.

The Trade Desk	https://www.humansecurity.com/newsroom/the-trade-desk-partners-with-white-ops-to-become-first-advertising-platform-to-block-fraudulent-impressions-before-they-are-purchased	8/31/2017

Microsoft Xandr	https://www.prnewswire.com/news-releases/appnexus-expands-inventory-quality-initiative-through-partnership-with-white-ops-300666958.html	6/15/2018
Index Exchange	https://www.humansecurity.com/newsroom/index-exchange-partners-with-white-ops	8/12/2020
Google	https://support.google.com/campaignmanager/answer/6076504?hl=en	N/A
Sovrn	https://www.humansecurity.com/newsroom/the-human-collective-grows-more-than-5x-since-april-launch	10/13/2021
Yieldmo	https://www.humansecurity.com/learn/blog/yieldmo-and-white-ops-ensuring-squeaky-clean-mobile-inventory	9/10/2019
Sharethrough	https://www.sharethrough.com/blog/sharethrough-founding-member-of-the-human-collective-in-effort-to-keep-ads-human	10/27/2021
Kargo	https://www.humansecurity.com/newsroom/kargos-curated-marketplace-boasts-less-than-0.3-of-invalid-traffic-following-implementation-of-white-ops-mediaguard	5/29/2019
Gumgum	https://www.businesswire.com/news/home/20190529005284/en/GumGum-Partners-with-White-Ops-to-Deliver-Comprehensively-Safe-Ad-Exchange	5/29/2019
Triplelift	https://www.humansecurity.com/newsroom/triplelift-and-white-ops-partner-to-fight-fraud-in-native-advertising	5/1/2018
Magnite	https://www.businesswire.com/news/home/20161220005758/en/Joint-Statement-From-White-Ops-CEO-and-Rubicon-Project-President-on-Successful-Efforts-Countering-Russian-Ad-Fraud	12/20/2016
Pubmatic	https://www.humansecurity.com/newsroom/pubmatic-partners-with-white-ops-to-fight-bot-fraud-and-drive-higher-transparency-in-video-inventory	12/5/2017
Sonobi	https://www.prnewswire.com/news-releases/sonobi-partners-with-human-formerly-white-ops-to-safeguard-platform-from-sophisticated-bot-fraud-301286928.html	5/11/2021
Freewheel	https://www.humansecurity.com/newsroom/freewheel-and-white-ops-expand-partnership-globally-to-further-deepen-trust-in-premium-video-inventory	4/29/2020
Media.net	https://www.humansecurity.com/newsroom/white-ops-media.net-partnership-extends-pre-bid-fraud-protection-for-brands	5/15/2019
Beachfront	https://www.humansecurity.com/newsroom/white-ops-beachfront	5/15/2018
Primis	https://www.humansecurity.com/newsroom/primis-expands-partnership-with-white-ops-in-fight-against-fraud-to-create-a-clean-and-trusted-video-supply-chain	9/1/2020
Omnicom	https://www.humansecurity.com/newsroom/human-formerly-white-ops-launches-the-human-collective-to-protect-against-bot-attacks-and-fraud-across-advertising-supply-chain	4/14/2021

In the bar chart below, one can see the relative number of ad impressions served on behalf of various advertisers using the Trade Desk to bots in the data sample via various supply side platforms, ad exchanges, and integrations. The largest relative number of ads purchased via Trade Desk DSP that were served to bots in the data sample were transacted via Trade Desk Open Path. Trade Desk Open Path was observed serving ads to bots on behalf of brands such as the Government of DC, US Hershey's, US Bank, Progressive, Procter & Gamble (P&G), Hershey's, WideOpenWest Finance, Kimberly Clark, Samsung, UPS, Coca-Cola, Walmart, McDonald's, and others.


Which SSPs Were Seen Serving the Highest Number of Trade Desk DSP Ads to Bots

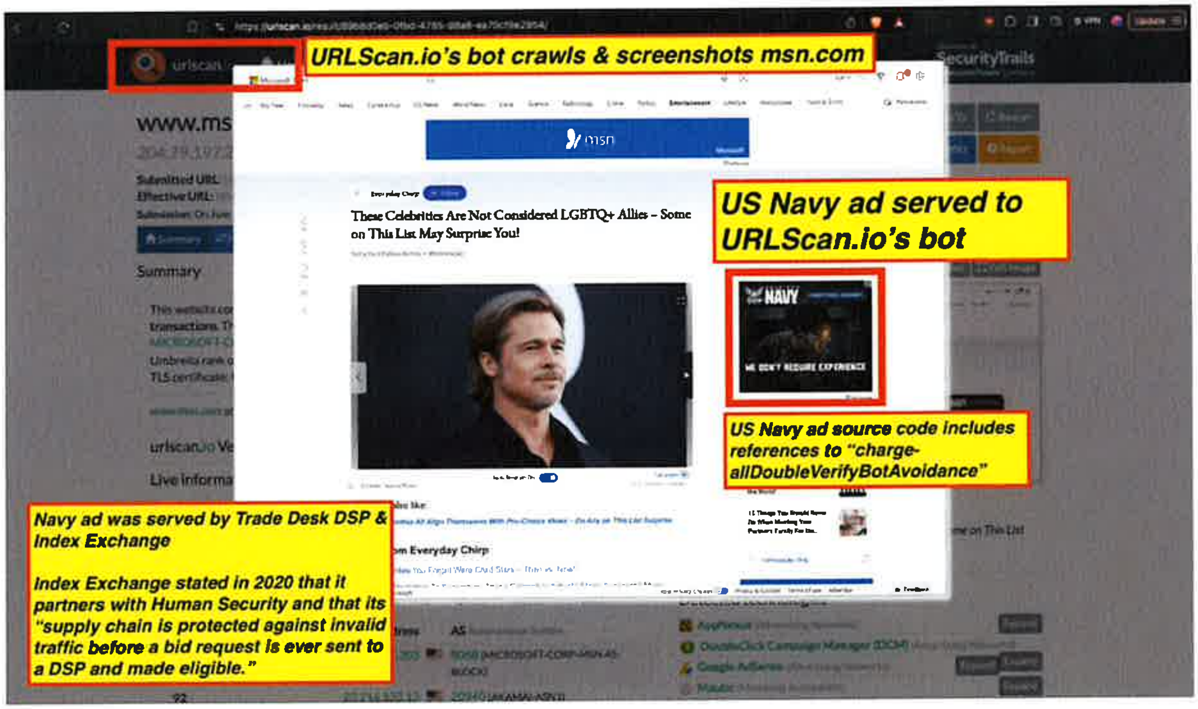
Bold Dark Blue label indicates SSP has announced partnering with Human Security (f/k/a) White Ops

Data based on bot data from 2019-2024 from URLscan.io and HTTP Archive

The second largest relative number of Trade Desk DSP ads served to bots in the sample were transacted by Microsoft Xandr SSP. Xandr has issued multiple announcements about partnering with HUMAN Security (f/k/a White Ops). Xandr was observed serving Trade Desk DSP ads to declared bots (whose user agent is on the IAB Tech Labs Bots & Spider

List since 2013) operating out of known data center IP address on behalf of advertisers such as Procter & Gamble, Target, Sling, US Bank, MasterCard, Starbucks, UPS, T-Mobile, Progressive, Pfizer, Ally, Nestle, Cox, Walamrt, Hilton, Unilever, Haleon, Hersheys, Coca-Cola, the Government of Utah, Samsung, and many others.

The third largest relative number of Trade Desk DSP ads served to bots in the sample were transacted by Index Exchange SSP. Index Exchange has issued multiple announcements about partnering with HUMAN Security (f/k/a White Ops), stating that the partnership allows advertisers to buy "with confidence that its supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible." Index Exchange was observed serving Trade Desk DSP ads to declared bots (whose user agent is on the IAB Tech Labs Bots & Spider List since 2013) operating out of known data center IP address on behalf of media agencies such as Omnicom, GroupM, MiQ and advertisers such as the United States Navy, the Government of DC, Kenvue, Progressive, US Bank, Hersheys, Procter & Gamble, T-Mobile, Target, Kimberly-Clark, Walmart, the Government of DC, Nestle, Coca-Cola, Pizza Hut, State Farm, Starbucks, American Airlines, Apple, Jimmy Dean, Mars, H&R BLock, Haleon, Bayer, Unilever, Volkswagen, Novo Nordisk, and many others.



urlscan
www.ms
msn
These Celebrities Are Not Considered LGBTQ+ Allies – Some on This List May Surprise You!
NAVY
SecurityTrails
Summary

URLScan.io's bot crawls & screenshots msn.com

US Navy ad served to URLScan.io's bot

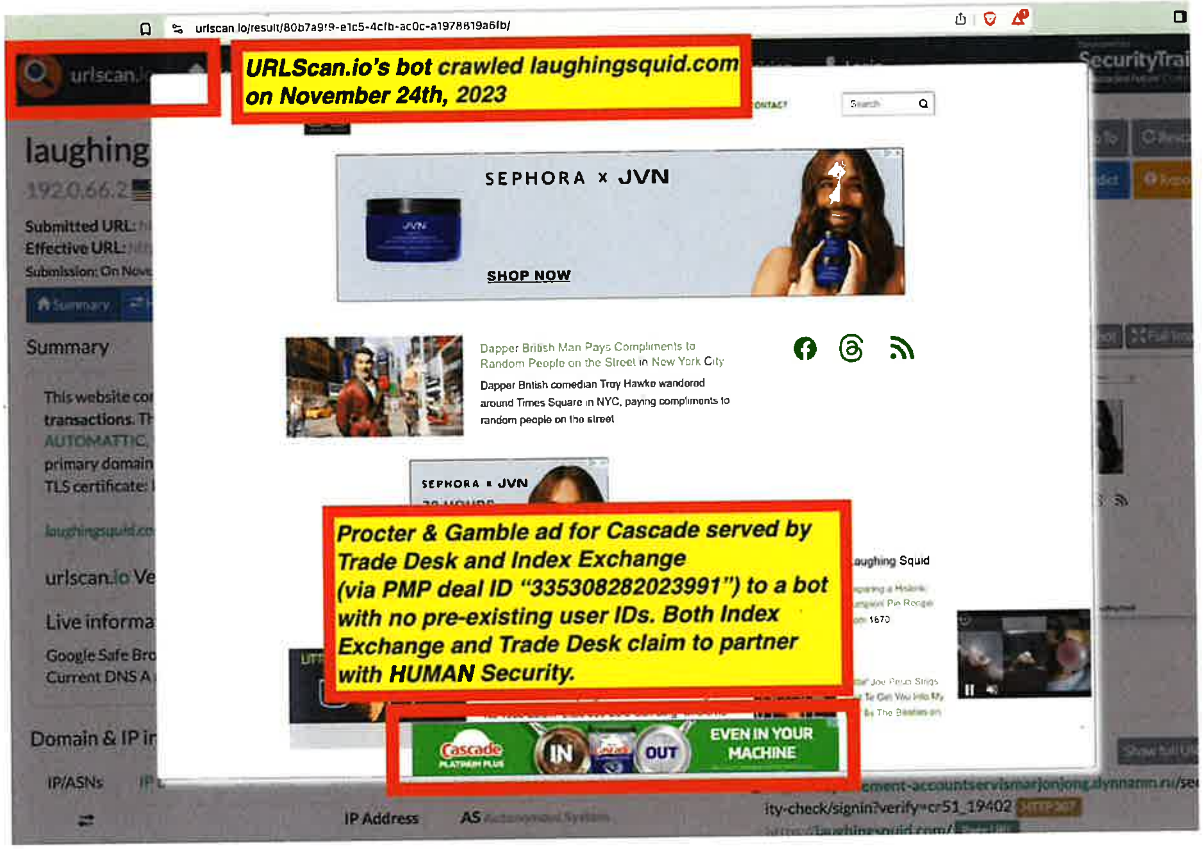
US Navy ad source code includes references to "charge-allDoubleVerifyBotAvoidance"

Navy ad was served by Trade Desk DSP & Index Exchange

Index Exchange stated in 2020 that it partners with Human Security and that its "supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible."

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Screenshot of URLScan.io's website, showing a URLScan.io bot crawl from June 16th, 2023. One can see a US Navy ad that was mediated by Trade Desk, Index Exchange, DoubleVerify, and/or HUMAN Security on msn.com.



URLScan.io's bot crawled laughingsquid.com on November 24th, 2023

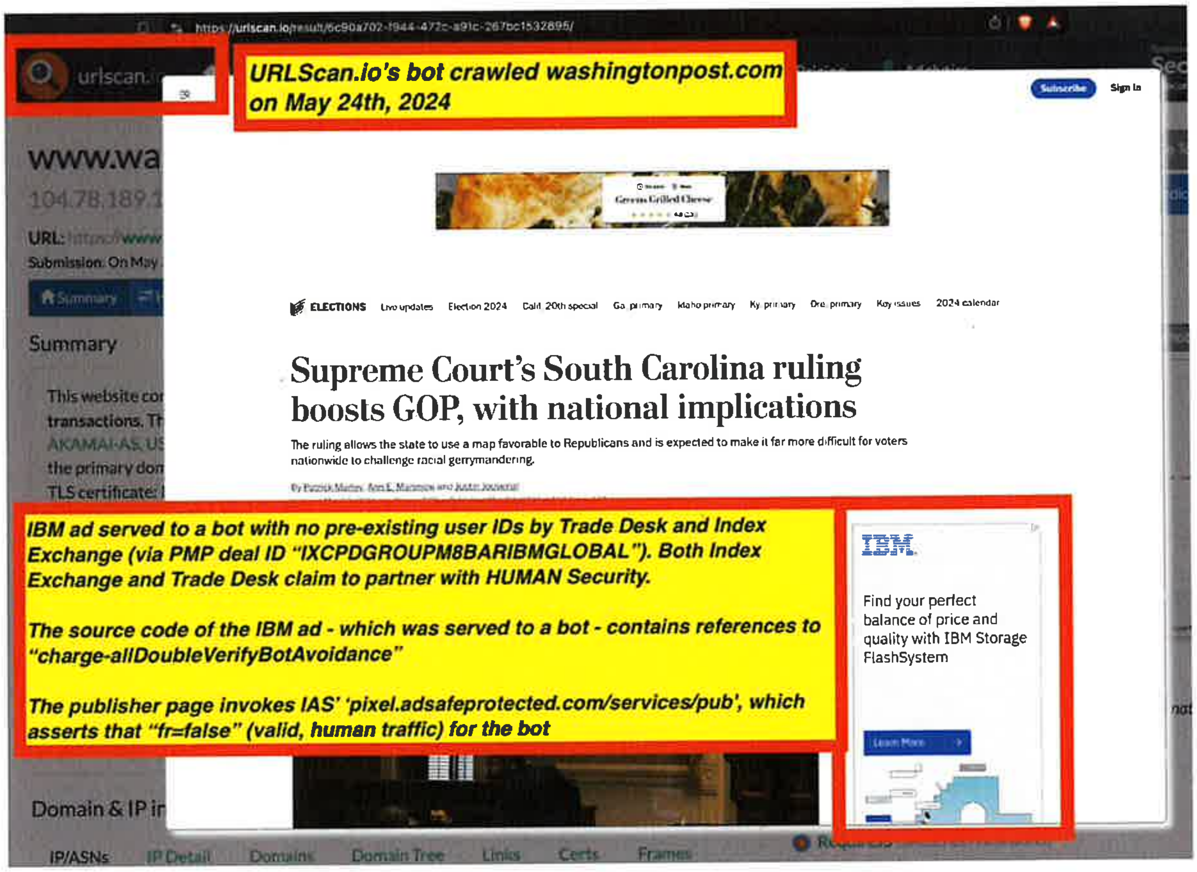
Procter & Gamble ad for Cascade served by Trade Desk and Index Exchange (via PMP deal ID "335308282023991") to a bot with no pre-existing user IDs. Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

urlscan.io/result/80b7a9f9-e1c5-4cfb-ac0c-a1978819a6fb/
urlscan.io
laughing
Submitted URL:
Effective URL:
Submission: On Nov
Summary
SEPHORA × JVN
SHOP NOW
Dapper British Man Pays Compliments to Random People on the Street in New York City
Dapper British comedian Troy Hawke wandered around Times Square in NYC, paying compliments to random people on the street
Cascade PLATINUM PLUS
IN
OUT
EVEN IN YOUR MACHINE
Domain & IP in
IP/ASNs
IP Address
AS

Screenshot of a Procter & Gamble ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "335308282023991"). URLScan source: https://urlscan.io/result/80b7a9f9-e1c5-4cfb-ac0c-a1978819a6fb/

Some of the Trade Desk ads that Index Exchange transacted to declared bots in data centers appear to have been transacted via PMP deal IDs. For examples, Index Exchange appeared to transacted Trade Desk ads to declared bots on behalf of Home Instead (PMP deal ID "OMGIXMARKETPLACEVIDEO2020"), Statefarm (PMP deal ID "OMGIXMARKETPLACEDISPLAY2020"), Apple (PMP deal "OMGIXMARKETPLACEDISPLAY2020"), and Hallmark ("OMGIXMARKETPLACEDISPLAY2020" and "OMGIXMARKETPLACEVIDEO2020"). Index Exchange also appeared to transacted Trade Desk ads to declared bots in data centers on behalf of T-Mobile (PMP deal IDs "IXCPDTTDTMOBILEDESK", "IXCPDTTDTMOBILEMOBAPP", "IXCPDTTDTMOBILEMOBW", "IXCPDTTDTMOBILEOUT", and others), Kimberly-Clark (PMP deal IDs "IXCPDMSKCTTDDIS"), Walmart (PMP deal IDs "IXIVPWMRTTECHFSHNDIS ", "IXIVPWMRTFAMBGTDIS", "IXCPDTTDUSADISPLAYNATIVEFINANCE", and others), Coca-Cola (PMP deal IDs "IXIVPCOCACOLA" and "IXIVPCOCACOLARONVIDEO"), Bayer (PMP deal ID "IXCPDBAYERDIS001"), Jimmy Dean (PMP deal ID "GROUPMIXFLOOR1SHEMEDIA"), Unilever (PMP deal IDs "IXIVPUNILEVERHISMOB", "IXIVPUNILEVERHISDIS", "IX621858871749986750", and others), and Mars (PMP deal ID "IXIVPTTDMARSAAOLV").

For example, in the screenshot below one can observe an IBM ad that was served to URLScan.io's bot on May 24th, 2024 whilst crawling washingtonpost.com. The IBM ad appears to have been transacted by GroupM media agency, Trade Desk, and Index Exchange (via PMP deal ID "IXCPDGROUPM8BARIBMGLOBAL"). The source code of the IBM ad includes references to "*charge-allDoubleVerifyBotAvoidance*", and code from DoubleVerify. IAS' publisher optimization tool was installed on washingtonpost.com, and classified the URLScan.io bot as "fr=false" (valid, human traffic).



https://urlscan.io/result/6c90a702-f944-472c-a91c-267bc1532895/

URLScan.io's bot crawled washingtonpost.com on May 24th, 2024

Supreme Court's South Carolina ruling boosts GOP, with national implications

The ruling allows the state to use a map favorable to Republicans and is expected to make it far more difficult for voters nationwide to challenge racial gerrymandering.

IBM ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "IXCPDGROUPM8BARIBMGLOBAL"). Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

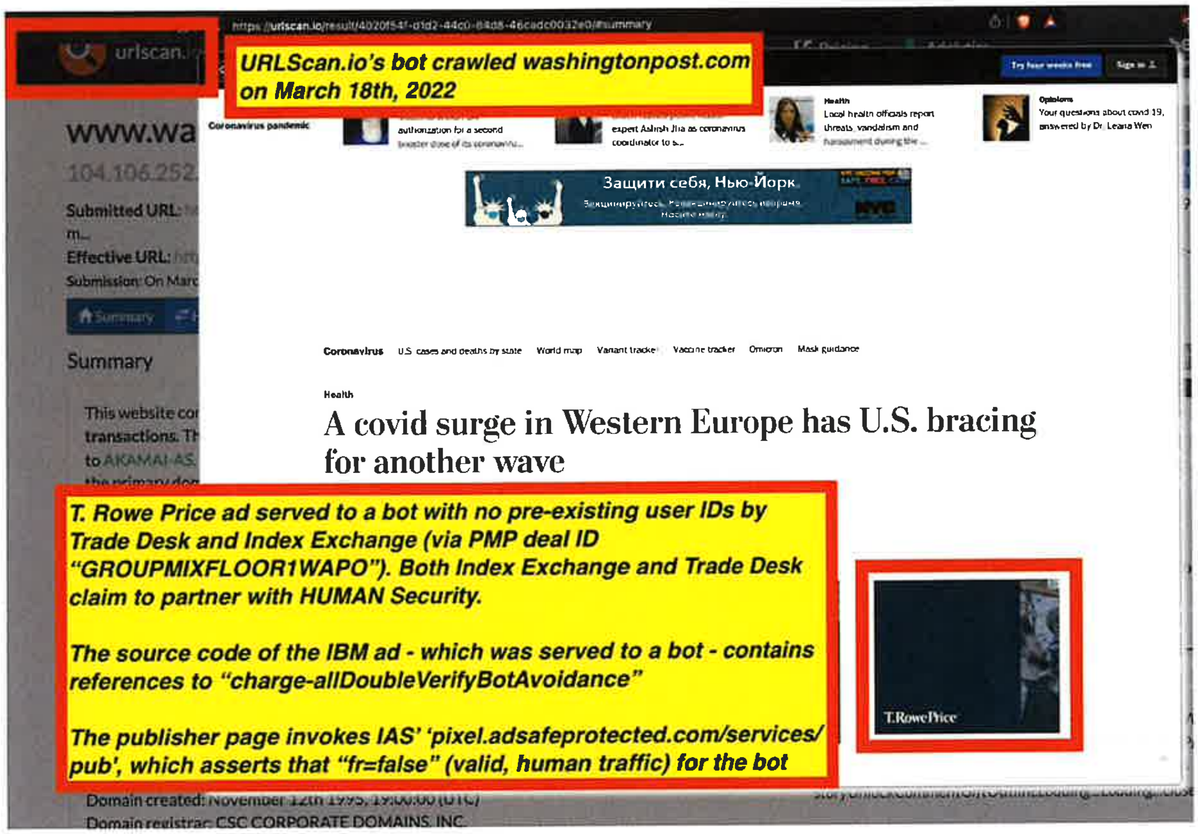
The source code of the IBM ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

The publisher page invokes IAS' 'pixel.adsafeprotected.com/services/pub', which asserts that "fr=false" (valid, human traffic) for the bot

IBM
Find your perfect balance of price and quality with IBM Storage FlashSystem
Learn More

Screenshot of an IBM ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "IXCPDGROUPM8BARIBMGLOBAL"). The source code of the IBM ad includes references to "charge-allDoubleVerifyBotAvoidance". The publisher's website invokes the IAS endpoint "pixel.adsafeprotected.com/services/pub", which returns the classification ("fr=false", meaning valid, human traffic). URLScan source: https://urlscan.io/result/6c90a702-f944-472c-a91c-267bc1532895/

As another example, in the screenshot below one can observe an T. Rowe Price ad that was served to URLScan.io's bot on March 18th, 2022 whilst crawling washingtonpost.com. The T. Rowe Price ad appears to have been transacted by GroupM media agency, Trade Desk, and Index Exchange (via PMP deal ID "GROUPMIXFLOOR1WAPO"). The source code of the T. Rowe Price ad includes references to "charge-allDoubleVerifyBotAvoidance", and code from DoubleVerify. IAS' publisher optimization tool was installed on washingtonpost.com, and classified the URLScan.io bot as "fr=false" (valid, human traffic).



URLScan.io's bot crawled washingtonpost.com on March 18th, 2022

T. Rowe Price ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "GROUPMIXFLOOR1WAPO"). Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

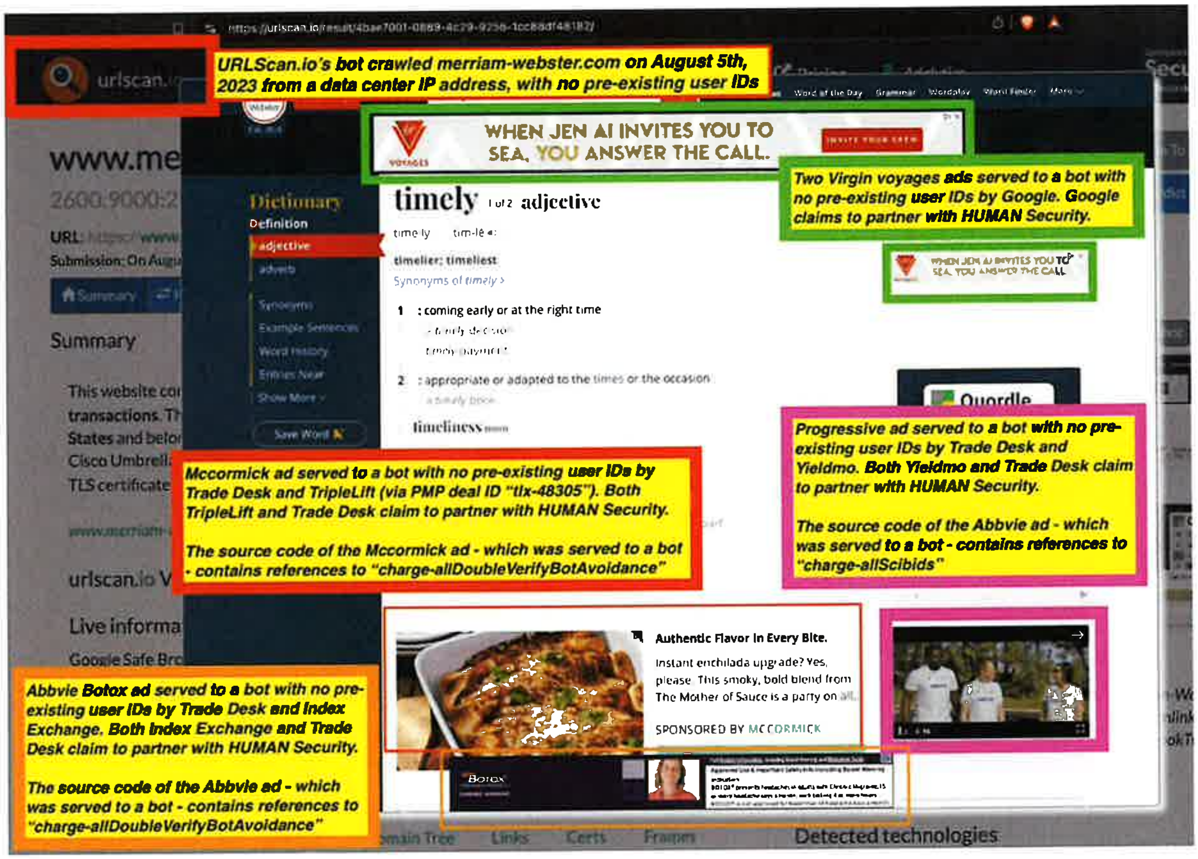
The source code of the IBM ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

The publisher page invokes IAS' 'pixel.adsafeprotected.com/services/pub', which asserts that "fr=false" (valid, human traffic) for the bot

https://urlscan.io/result/4020f54f-d1d2-44c0-84d8-46cadc0032e0/#summary
urlscan.io
www.wa
104.106.252.
Submitted URL:
Effective URL:
Submission: On Marc
Summary
Summary
This website co
transactions. Th
to AKAMAI-AS.
Domain created: November 12th 1995, 19:00:00 (UTC)
Domain registrar: CSC CORPORATE DOMAINS, INC.
Try four weeks free
Sign in
Coronavirus pandemic
authorization for a second booster dose of its coronavirus...
expert Ashish Jha as coronavirus coordinator to s...
Health
Local health officials report threats, vandalism and harassment during the ...
Opinions
Your questions about covid 19, answered by Dr. Leana Wen
Защити себя, Нью-Йорк
NYC
Coronavirus
U.S. cases and deaths by state
World map
Variant tracker
Vaccine tracker
Omicron
Mask guidance
Health
A covid surge in Western Europe has U.S. bracing for another wave
T.RowePrice

Screenshot of a T. Rowe Price ad served to a bot with no pre-existing user IDs by GroupM, Trade Desk, and Index Exchange (via PMP deal ID "GROUPMIXFLOOR1WAPO"). The source code of the IBM ad includes references to "charge-allDoubleVerifyBotAvoidance". The publisher's website invokes the IAS endpoint "pixel.adsafeprotected.com/services/pub", which returns the classification ("fr=false", meaning valid, human traffic). URLScan source: https://urlscan.io/result/4020f54f-d1d2-44c0-84d8-46cadc0032e0/

As another example, in the screenshot below one can observe an Abbvie Botox ad, a Progressive insurance ad, and a Mccormick ad that were served to URLScan.io's bot on August 5th, 2023 whilst crawling merriam-webster.com. The Abbvie Botox ad appears to have been transacted by Trade Desk and Index Exchange, and its source code includes references to "charge-allDoubleVerifyBotAvoidance". The Mccormick ad appears to have been transacted by Trade Desk and Triplelift (via PMP deal ID "tlx-48305"), and its source code includes references to "charge-allDoubleVerifyBotAvoidance". The Progressive insurance ad appears to have been transacted by Trade Desk and Yieldmo, and its source code includes references to Scibids. Two Virgin Voyages ads were also served to the bot and appear to have been transacted by Google DV360.



URLScan.io's bot crawled merriam-webster.com on August 5th, 2023 from a data center IP address, with no pre-existing user IDs

Two Virgin voyages ads served to a bot with no pre-existing user IDs by Google. Google claims to partner with HUMAN Security.

Mccormick ad served to a bot with no pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-48305"). Both TripleLift and Trade Desk claim to partner with HUMAN Security.

The source code of the Mccormick ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

Progressive ad served to a bot with no pre-existing user IDs by Trade Desk and Yieldmo. Both Yieldmo and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allScibids"

Abbvie Botox ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange. Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

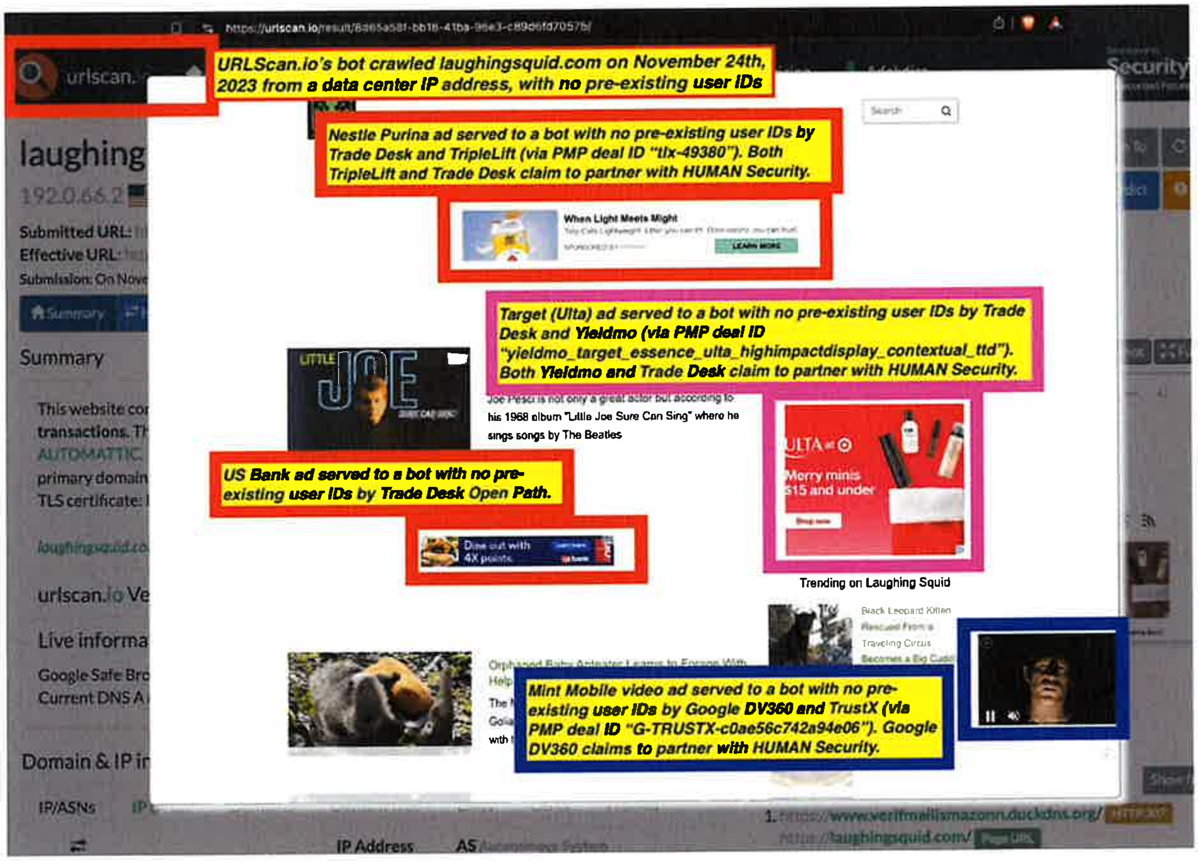
Multiple DV360 and Trade Desk ads served to URLScan.io's bot, which was operating out of a data center with no pre-existing user IDs whilst crawling merriam-webster.com on August 5th, 2023. The bot was served two ads for Virgin Voyages by Google, and ads for Mccormick, Progressive, and Abbvie botox. The Mccormick and Abbvie ads' source code contains references to "charge-allDoubleVerifyBotAvoidance", whilst the Progressive video ad contains references to "charge-allScibids". The ads were transacted by Yieldmo, Index Exchange, and TripleLift (via PMP deal ID "tlx-48305"), all of whom have many public statements about partnering with HUMAN Security. Source: https://urlscan.io/result/4bae7001-0889-4c29-9256-1cc88df48182/

As another example, in the screenshot below one can observe an Nestle Purina ad, a US Bank ad, a Target (Ulta) ad, and a Mint Mobile that were served to URLScan.io's bot on November 24th, 2023 whilst crawling laughingsquid.com.

The Nestle Purina ad appears to have been transacted by Trade Desk and Triplelift (via PMP deal ID "tlx-49380"). The US Bank ad appears to have been transacted by Trade Desk Open Path.

The Target (Ulta) ad appears to have been transacted by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_target_essenc_ulta_highimpactdisplay_contextual_ttd").

A Mint Mobile ad appears to have been transacted by Google DV360 and TrustX (via PMP deal ID "G-TRUSTX-c0ae56c742a94e06").



URLScan.io's bot crawled laughingsquid.com on November 24th, 2023 from a data center IP address, with no pre-existing user IDs

Nestle Purina ad served to a bot with no pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-49380"). Both TripleLift and Trade Desk claim to partner with HUMAN Security.

Target (Ulta) ad served to a bot with no pre-existing user IDs by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_target_essence_ulta_highimpactdisplay_contextual_ttd"). Both Yieldmo and Trade Desk claim to partner with HUMAN Security.

US Bank ad served to a bot with no pre-existing user IDs by Trade Desk Open Path.

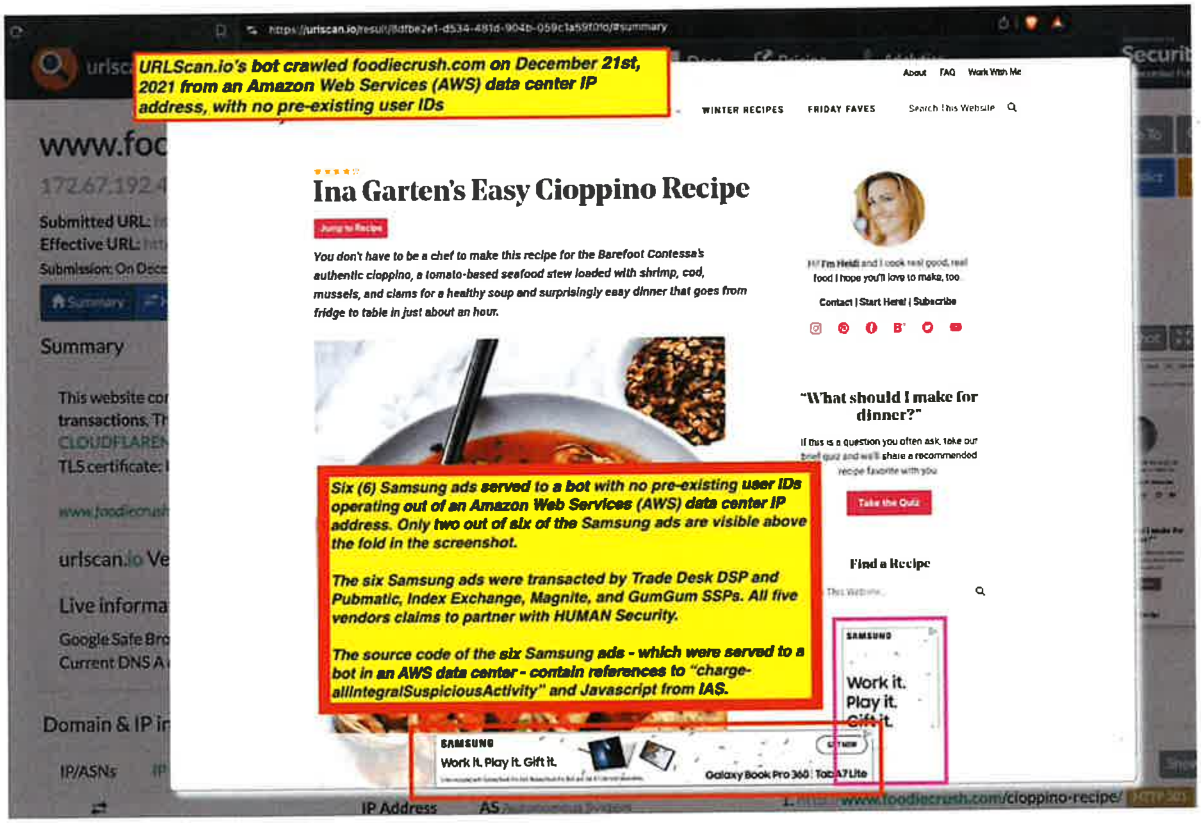
Mint Mobile video ad served to a bot with no pre-existing user IDs by Google DV360 and TrustX (via PMP deal ID "G-TRUSTX-c0ae56c742a94e06"). Google DV360 claims to partner with HUMAN Security.

https://urlscan.io/result/8a65a581-bb18-41ba-96e3-c89d6fd7057b/
urlscan.
laughing
192.0.66.2
Submitted URL:
Effective URL:
Submission: On Nove
Summary
Summary
This website co
transactions. Th
AUTOMATTIC
primary domain
TLS certificate:
urlscan.io Ve
Live informa
Google Safe Bro
Current DNS A
Domain & IP in
IP/ASNs
IP Address
AS Autonomous System
Search
When Light Meets Might
LEARN MORE
LITTLE JOE
Joe Pesci is not only a great actor but according to his 1968 album "Little Joe Sure Can Sing" where he sings songs by The Beatles
ULTA
Merry minis $15 and under
Dine out with 4X points
Trending on Laughing Squid
Black Leopard Kitten Rescued From a Traveling Circus Becomes a Big Cuddler
Orphaned Baby Anteater Learns to Forage With Help
Security
1. https://www.verifmailismazonn.duckdns.org/
https://laughingsquid.com/

Multiple DV360 and Trade Desk ads served to URLScan.io's bot, which was operating out of a data center with no pre-existing user IDs whilst crawling laughingsquid.com on November 23rd, 2023. The bot was served a Mint Mobile video ad by DV360 and TrustX (via PMP deal ID "G-TRUSTX-c0ae56c742a94e06"). The bot was also served ads for Nestle

Purina, US Bank, and Target (Ulta). The ads were transacted by TripleLift (via PMP deal ID "tlx-49380"), Trade Desk Open Path, and Yieldmo (via PMP deal ID "yieldmo_target_essence_ulta_highimpactdisplay_contextual_ttd") respectively, all of whom have many public statements about partnering with HUMAN Security. Source: https://urlscan.io/result/8d65a58f-bb18-41ba-96e3-c89d6fd70575/

As another example, six Samsung ads were served to URLScan.io's bot whilst it was crawling foodiecrush.com on December 21st, 2021 from an Amazon Web Services (AWS) data center IP address with no pre-existing user IDs. Only two of the six Samsung ads are visible above-the-fold in the screenshot. The six Samsung ads were transacted by Trade Desk, Index Exchange, Pubmatic, Magnite, and Gumgum. All five vendors claim to partner with HUMAN Security. The source code of the Samsung ads includes references to "charge-allIntegralSuspiciousActivity" and Javascript from IAS.



https://urlscan.io/result/8dfbe2e1-d534-481d-904b-059c1a59f0f0/#summary

URLScan.io's bot crawled foodiecrush.com on December 21st, 2021 from an Amazon Web Services (AWS) data center IP address, with no pre-existing user IDs

Ina Garten's Easy Cioppino Recipe

You don't have to be a chef to make this recipe for the Barefoot Contessa's authentic cioppino, a tomato-based seafood stew loaded with shrimp, cod, mussels, and clams for a healthy soup and surprisingly easy dinner that goes from fridge to table in just about an hour.

Hi! I'm Heidi and I cook real good, real food I hope you'll love to make, too.

"What should I make for dinner?"

If this is a question you often ask, take our brief quiz and we'll share a recommended recipe favorite with you

Six (6) Samsung ads served to a bot with no pre-existing user IDs operating out of an Amazon Web Services (AWS) data center IP address. Only two out of six of the Samsung ads are visible above the fold in the screenshot.

The six Samsung ads were transacted by Trade Desk DSP and Pubmatic, Index Exchange, Magnite, and GumGum SSPs. All five vendors claims to partner with HUMAN Security.

The source code of the six Samsung ads - which were served to a bot in an AWS data center - contain references to "charge-allIntegralSuspiciousActivity" and Javascript from IAS.

[On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?](https://adalytics.io/blog/prebid-bot-filtration)

Six Samsung ads served by Trade Desk to URLScan.io's bot, which was operating out of an Amazon Web Services (AWS) data center with no pre-existing user IDs whilst crawling foodiecrush.com on December 21st, 2021. Only two of the six Samsung ads are visible above the viewport in the screenshot. The six Samsung ads were transacted by Pubmatic, Index Exchange, Magnite, and GumGum, all of whom have many public statements about partnering with HUMAN Security. The source code of the six Samsung ads that were served to a bot in an AWS data center contain references to "charge-allIntegralSuspiciousActivity" and Javascript from IAS. Source: https://urlscan.io/result/8dfbe2e1-d534-481d-904b-059c1a59f0fd/

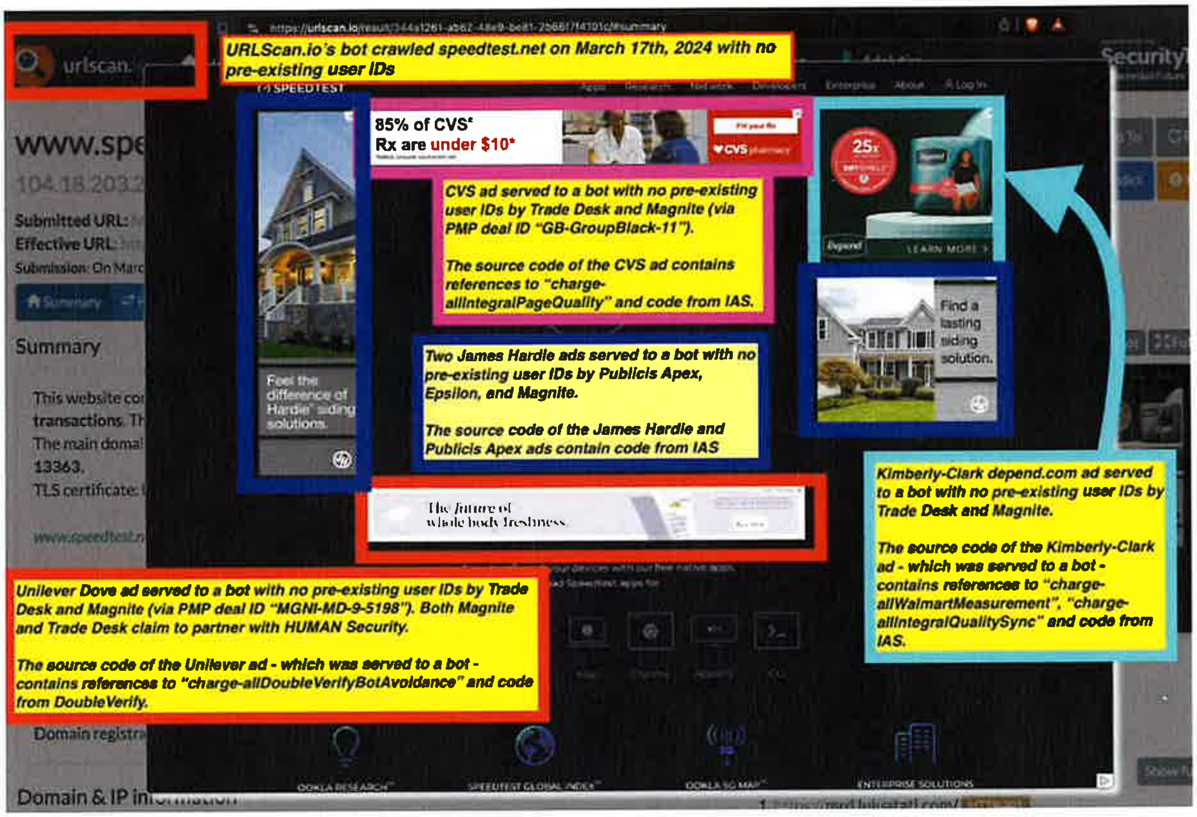
As another example, a CVS ad, a Kimberly-Clark Depend ad, a Unilever Dove ad, and two James Hardie ads were served to URLScan.io's bot whilst it was crawling speedtest.net on March 17th, 2024.

The CVS ad appears to have been transacted by Trade Desk and Magnite (via PMP deal ID "GB-GroupBlack-11), and its source code includes references to "charge-allIntegralPageQuality" and code from IAS.

The Kimberly-Clark Depend ad that was served to the bot appears to have been transacted by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security. The source code of the Kimberly-Clark ad includes reference to "charge-alllIntegralQualitySync" and code from IAS.

The Unilever Dove ad that was served to a bot appears to have been transacted by Trade Desk and Magnite (via PMP deal ID "MGNI-MD-9-5198"). The Unilever Dove ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

The two James Hardie ads that were served to the bot appear to have been transacted by Publicis-Groupe owned Epsilon and Magnite.The source code of the James Hardie ads includes references to "Apex". According to Ad Age, "Apex Exchange, is making principal investments in both traditional and digital media inventory that it then resells to clients [...] "We are very clear with clients where we've made an investment." Those clients waive their right to transparency on costs and fees." The James Hardie source code includes references to IAS.


urlscan.
https://urlscan.io/result/344a1261-ab62-48e9-be81-2b68f7f4101c/#summary
SPEEDTEST
www.spe
Submitted URL:
Effective URL:
Submission: On Marc
Summary
85% of CVS* Rx are under $10*
CVS pharmacy
25x
Depend
LEARN MORE
Feel the difference of Hardie® siding solutions.
Find a lasting siding solution.
The future of whole body freshness
OOKLA RESEARCH
SPEEDTEST GLOBAL INDEX
OOKLA 5G MAP
ENTERPRISE SOLUTIONS
Domain registra
Domain & IP in

URLScan.io's bot crawled speedtest.net on March 17th, 2024 with no pre-existing user IDs

CVS ad served to a bot with no pre-existing user IDs by Trade Desk and Magnite (via PMP deal ID "GB-GroupBlack-11").

The source code of the CVS ad contains references to "charge-allIntegralPageQuality" and code from IAS.

Two James Hardie ads served to a bot with no pre-existing user IDs by Publicis Apex, Epsilon, and Magnite.

The source code of the James Hardie and Publicis Apex ads contain code from IAS

Kimberly-Clark depend.com ad served to a bot with no pre-existing user IDs by Trade Desk and Magnite.

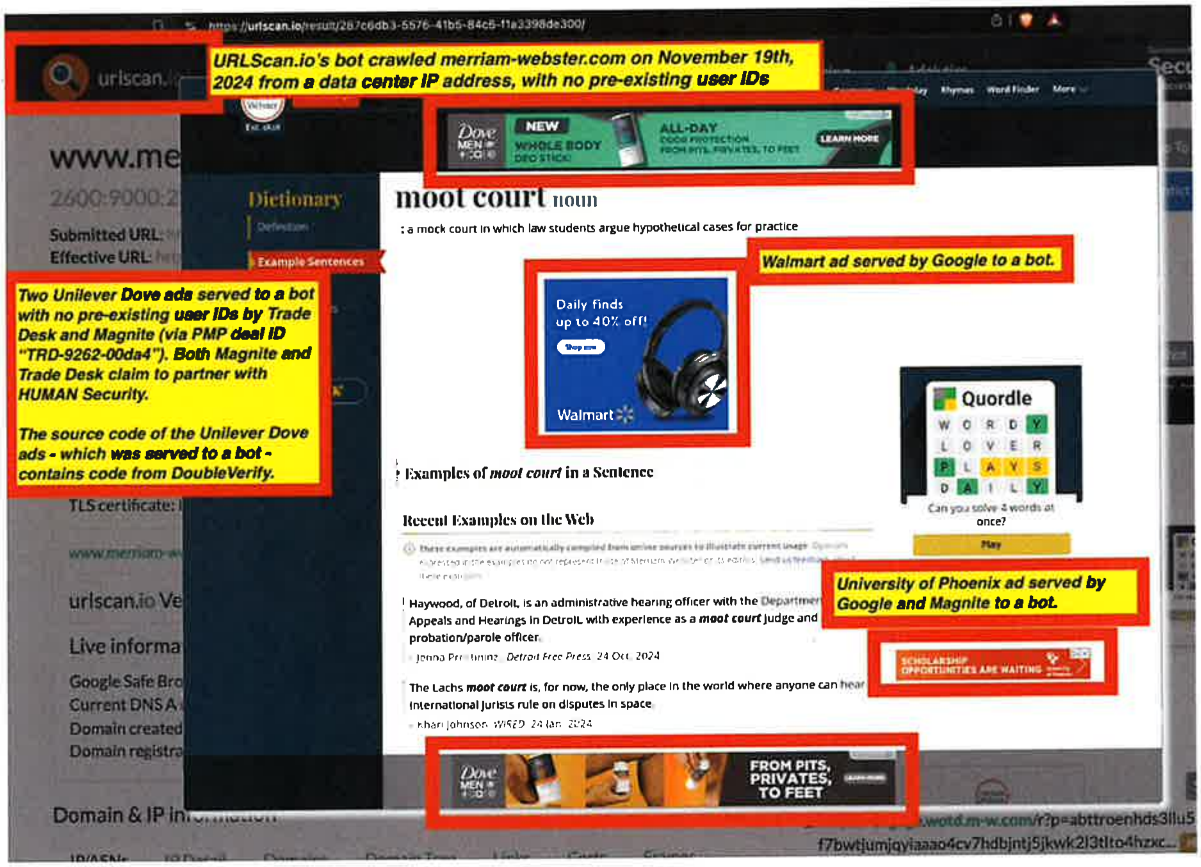
The source code of the Kimberly-Clark ad - which was served to a bot - contains references to "charge-allWalmartMeasurement", "charge-allIntegralQualitySync" and code from IAS.

Unilever Dove ad served to a bot with no pre-existing user IDs by Trade Desk and Magnite (via PMP deal ID "MGNI-MD-9-5198"). Both Magnite and Trade Desk claim to partner with HUMAN Security.

The source code of the Unilever ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

Multiple ads served by Trade Desk to URLScan.io's bot, which was operating with no pre-existing user IDs whilst crawling speedtest.com on March 17th, 2024. One Kimberly-Clark Depend ad was transacted by Magnite to the bot, and the source code of the Kimberly-Clark Depend ad includes references to "charge-allIntegralQualitySync". A Unilever Dove ad was transacted to the bot by Magnite via PMP deal ID "MGNI-MD-9-5198". The source code of the DoubleVerify ad that was served to a bot includes references to "charge-allDoubleVerifyBotAvoidance". A CVS ad transacted by Magnite to the bot via PMP deal ID "GB-GroupBlack-11". The source code of the CVS ad includes references to "charge-allIntegralPageQuality". In addition the three Trade Desk transacted ads, two ads for James Hardie were transacted by Publicis Groupe-owned Epsilon and Magnite. The source code of the James Hardie ads includes references to "Apex". According to Ad Age, "Apex Exchange, is making principal investments in both traditional and digital media inventory that it then resells to clients [...] "We are very clear with clients where we've made an investment." Those clients waive their right to transparency on costs and fees." The James Hardie source code *includes references to IAS.* Source: https://urlscan.io/result/344a1261-ab62-48e9-be81-2b66f7f4101c/

As another example, two Unilever Dove ads were served to URLScan.io's bot whilst it was crawling merriam-webster.com on November 19th, 2024 with no pre-existing user IDs. The two Unilever Dove ads were transacted by Trade Desk and Magnite (via PMP deal ID "TRD-9262-00da4"). The source code of the Unilever Dove ads includes code from DoubleVerify.



URLScan.io's bot crawled merriam-webster.com on November 19th, 2024 from a data center IP address, with no pre-existing user IDs

Two Unilever Dove ads served to a bot with no pre-existing user IDs by Trade Desk and Magnite (via PMP deal ID "TRD-9262-00da4"). Both Magnite and Trade Desk claim to partner with HUMAN Security.

The source code of the Unilever Dove ads - which was served to a bot - contains code from DoubleVerify.

Walmart ad served by Google to a bot.

University of Phoenix ad served by Google and Magnite to a bot.

moot court noun

: a mock court in which law students argue hypothetical cases for practice

Examples of *moot court* in a Sentence

Recent Examples on the Web

Haywood, of Detroit, is an administrative hearing officer with the Departmen[t] Appeals and Hearings in Detroit with experience as a *moot court* judge and probation/parole officer.

— Jenna Prestininzi, Detroit Free Press, 24 Oct. 2024

The Lachs *moot court* is, for now, the only place in the world where anyone can hear international jurists rule on disputes in space.

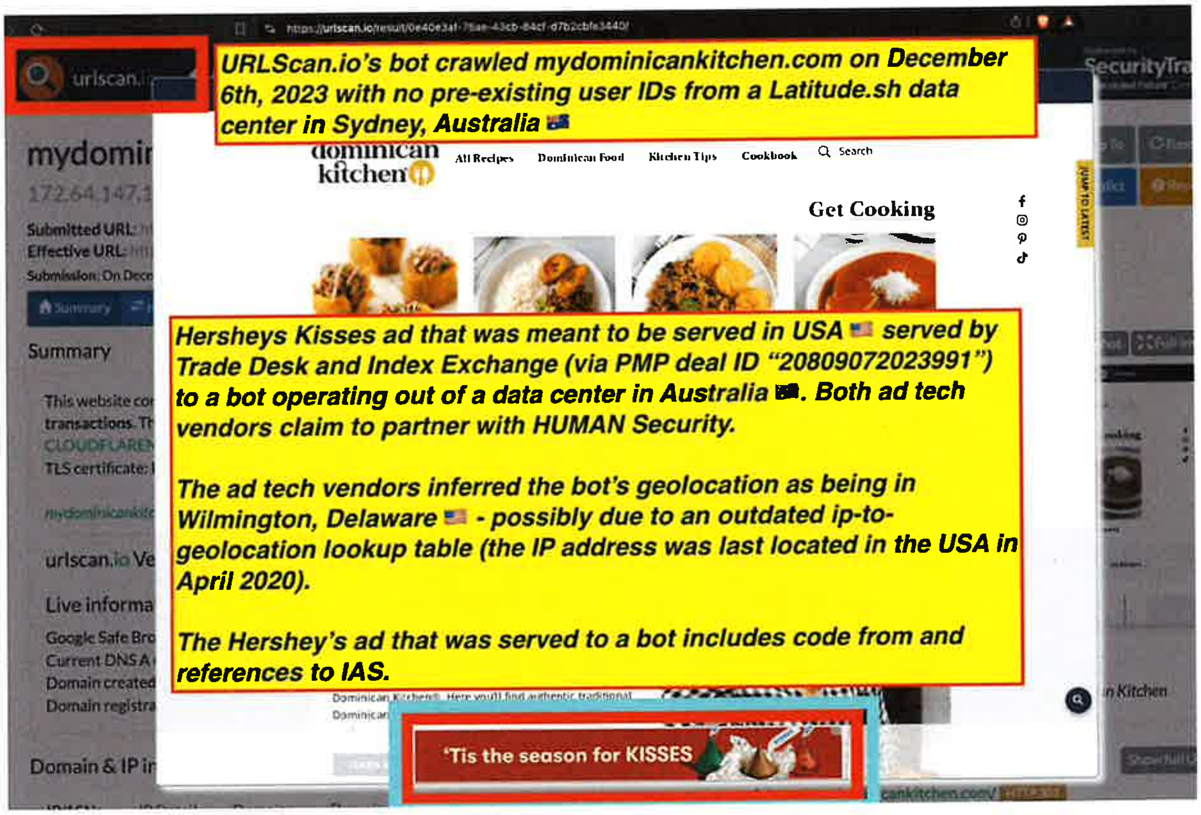
— Khari Johnson, WIRED, 24 Jan. 2024

https://urlscan.io/result/287c6db3-5576-41b5-84c6-f1a3398de300/
urlscan.io
www.me
2600:9000:2
Submitted URL:
Effective URL:
TLS certificate:
urlscan.io Ve
Live informa
Google Safe Bro
Current DNS A
Domain created
Domain registra
Domain & IP in
Dictionary
Definition
Example Sentences
Dove MEN+CARE
NEW
WHOLE BODY DEO STICK
ALL-DAY ODOR PROTECTION FROM PITS, PRIVATES, TO FEET
LEARN MORE
Daily finds up to 40% off!
Shop now
Walmart
Quordle
W O R D Y
L O V E R
P L A Y S
D A I L Y
Can you solve 4 words at once?
Play
SCHOLARSHIP OPPORTUNITIES ARE WAITING
FROM PITS, PRIVATES, TO FEET
wotd.m-w.com/r?p=abttroenhds3llu5
f7bwtjumjqyiaaao4cv7hdbjntj5jkwk2l3tlto4hzxc...

Two Unilever Dove ads served by Trade Desk to URLScan.io's bot, which was operating with no pre-existing user IDs whilst crawling merriam-webster.com on November 19th, 2024. The two Unilever Dove ads were transacted by Magnite (via PMP deal ID "TRD-9262-00da4"). The Unilever Dove ads contain code from DoubleVerify. One can also see ads for Walmart and University of Phoenix (transacted by Google). Source: https://urlscan.io/result/287c6db3-5576-41b5-84c6-f1a3398de300/

As another example, a Hershey's Kisses ad was served to URLScan.io's bot whilst it was crawling mydominicankitchen.com December 6th, 2023 with no pre-existing user IDs from a data center in Australia. The Hershey's Kisses ad was transacted by Trade Desk and Index Exchange (via PMP deal ID "20809072023991"), both of whom claim to partner with HUMAN Security. The source code of the Hershey's ad includes references to IAS.

The Hershey's ad appears to have been targeted to a consumer in Wilmington, Delaware, USA, but was served to a bot in a data center in Australia. This may be due to an outdated ip-to-geolocation lookup database used by one of the ad tech vendors.



URLScan.io's bot crawled mydominicankitchen.com on December 6th, 2023 with no pre-existing user IDs from a Latitude.sh data center in Sydney, Australia 🇦🇺

Hersheys Kisses ad that was meant to be served in USA 🇺🇸 ***served by Trade Desk and Index Exchange (via PMP deal ID "20809072023991") to a bot operating out of a data center in Australia*** 🇦🇺***. Both ad tech vendors claim to partner with HUMAN Security.***

The ad tech vendors inferred the bot's geolocation as being in Wilmington, Delaware 🇺🇸 ***- possibly due to an outdated ip-to-geolocation lookup table (the IP address was last located in the USA in April 2020).***

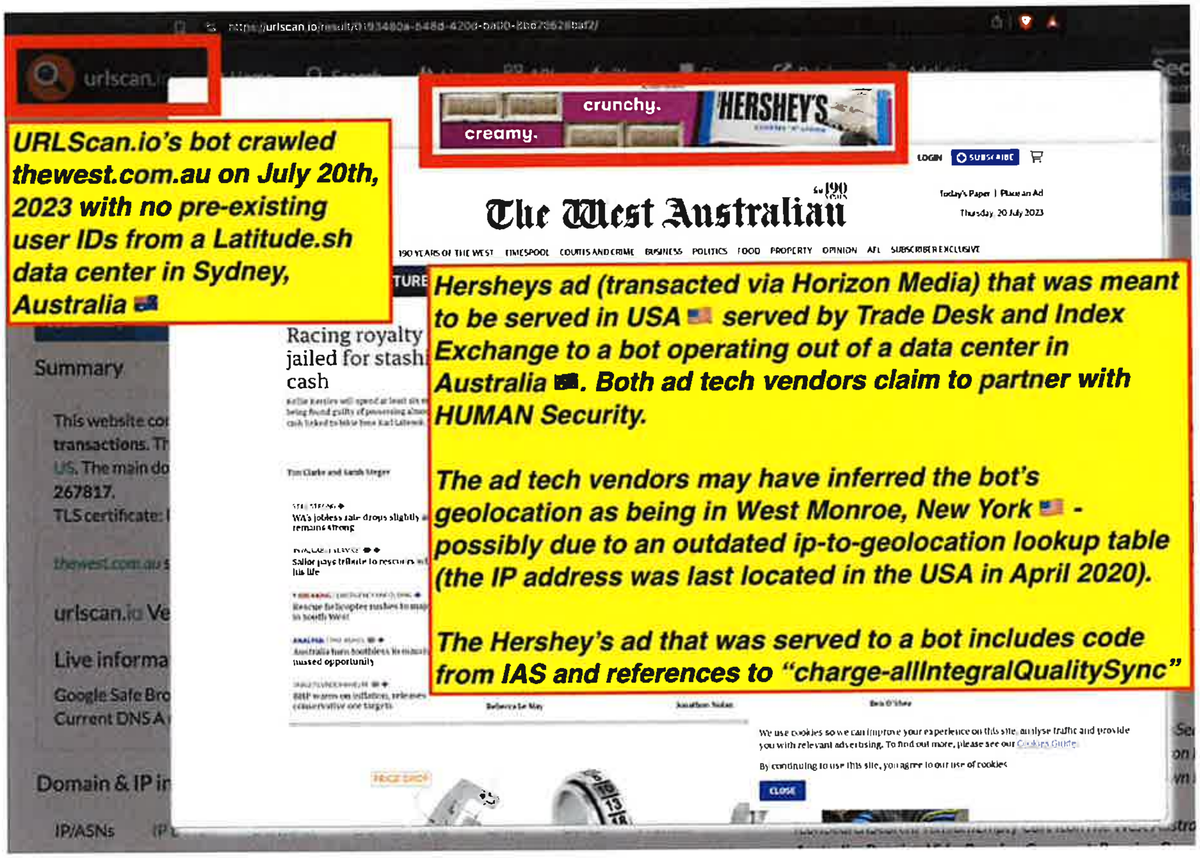
The Hershey's ad that was served to a bot includes code from and references to IAS.

URLScan.io's bot crawled mydominicankitchen.com on December 6th, 2023 with no pre-existing user IDs from a Latitude.sh data center in Sydney, Australia AU ; Hersheys Kisses ad that was meant to be served in USA US served by Trade Desk and Index Exchange (via PMP deal ID "20809072023991") to a bot operating out of a data center in Australia AU. Both ad tech vendors claim to partner with HUMAN Security. The ad tech vendors inferred the bot's geolocation as being in Wilmington, Delaware US - possibly due to an outdated ip-to-geolocation lookup table (the IP address was last located in the USA in April 2020). The Hershey's ad that was served to a bot includes code from and references to IAS.

https://urlscan.io/result/0e40e3af-76ae-43cb-84cf-d7b2cbfe3440/#summary

As another example, a Hershey's ad was served to URLScan.io's bot whilst it was crawling thewest.com.au on July 20th, 2023 with no pre-existing user IDs from a data center in Australia. The Hershey's ad was transacted by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security. The source code of the Hershey's ad includes references to IAS and "charge-allIntegralQualitySync".

The Hershey's ad appears to have been targeted to a consumer in West Monroe, New York, USA, but was served to a bot in a data center in Australia. This may be due to an outdated ip-to-geolocation lookup database used by one of the ad tech vendors.



URLScan.io's bot crawled thewest.com.au on July 20th, 2023 with no pre-existing user IDs from a Latitude.sh data center in Sydney, Australia 🇦🇺

Hersheys ad (transacted via Horizon Media) that was meant to be served in USA 🇺🇸 served by Trade Desk and Index Exchange to a bot operating out of a data center in Australia 🇦🇺. Both ad tech vendors claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in West Monroe, New York 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup table (the IP address was last located in the USA in April 2020).

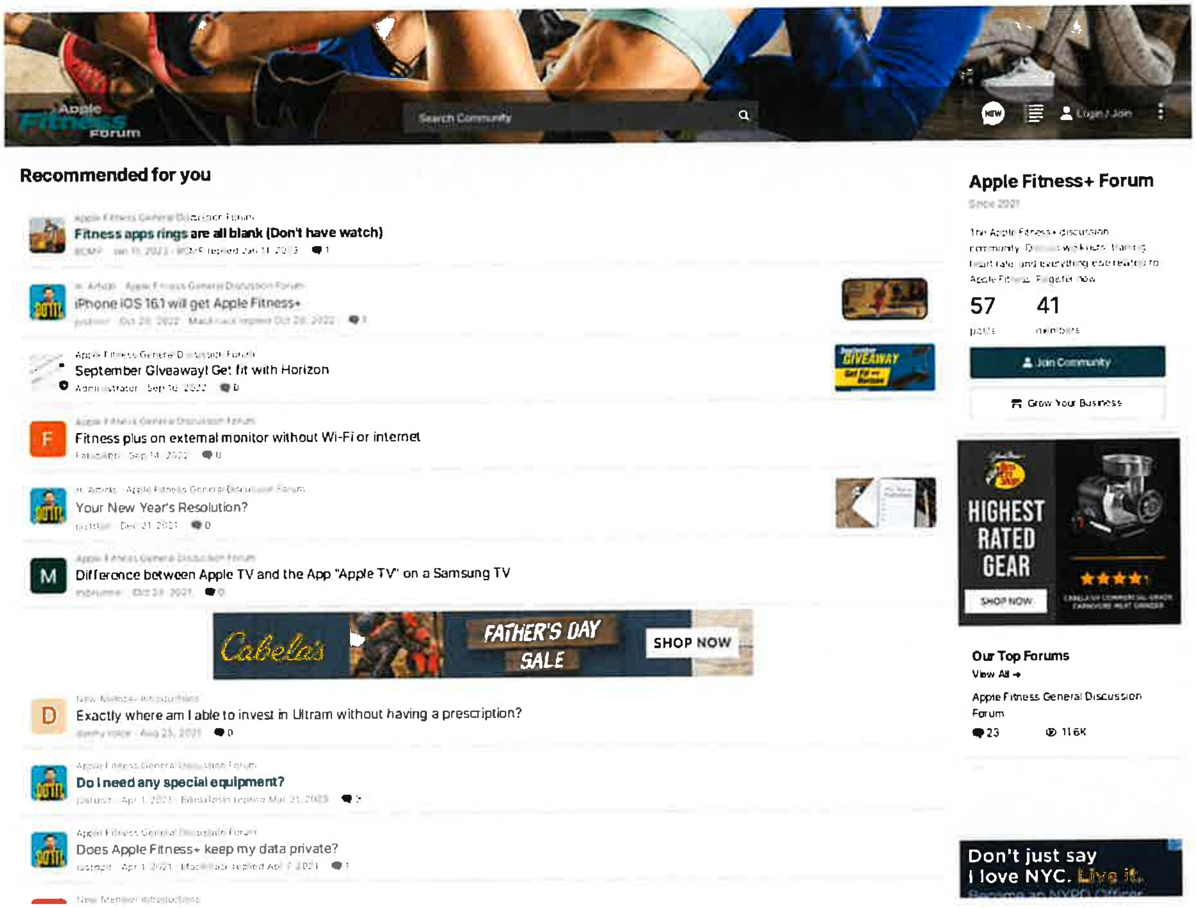
The Hershey's ad that was served to a bot includes code from IAS and references to "charge-allIntegralQualitySync"

URLScan.io's bot crawled thewest.com.au on July 20th, 2023 with no pre-existing user IDs from a Latitude.sh data center in Sydney, Australia AU. Hershey's ad (transacted via Horizon Media) that was meant to be served in USA US served by Trade Desk and Index Exchange to a bot operating out of a data center in Australia AU. Both ad tech vendors claim to partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in West Monroe, New York US - possibly due to an outdated ip-to-geolocation lookup table (the IP address was last located in the USA in April 2020). The Hershey's ad that was served to a bot includes code from IAS and references to "charge-allIntegralQualitySync".

https://urlscan.io/result/0193480a-548d-420d-ba00-8b676628baf2/#summary

As another example, in the screenshot below one can see an instance where New York City Police (NYPD) ads were served to URLScan.io's bot on June 2, 2024 whilst the bot was crawling applefitnessforum.co

(URLScan.io link: https://urlscan.io/result/37d33b15-1345-4637-a664-86897279f57b/). The ad was transacted by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.



Recommended for you

Apple Fitness General Discussion Forum
Fitness apps rings are all blank (Don't have watch)
1

iPhone iOS 16.1 will get Apple Fitness+
1

Apple Fitness General Discussion Forum
September Giveaway! Get fit with Horizon
Administrator · 0

Fitness plus on external monitor without Wi-Fi or internet
0

Your New Year's Resolution?
0

Difference between Apple TV and the App "Apple TV" on a Samsung TV
0

Exactly where am I able to invest in Ultram without having a prescription?
0

Do I need any special equipment?

Does Apple Fitness+ keep my data private?

Apple Fitness+ Forum

57 posts 41 members

Our Top Forums
View All →

Apple Fitness General Discussion Forum
23 11.6K

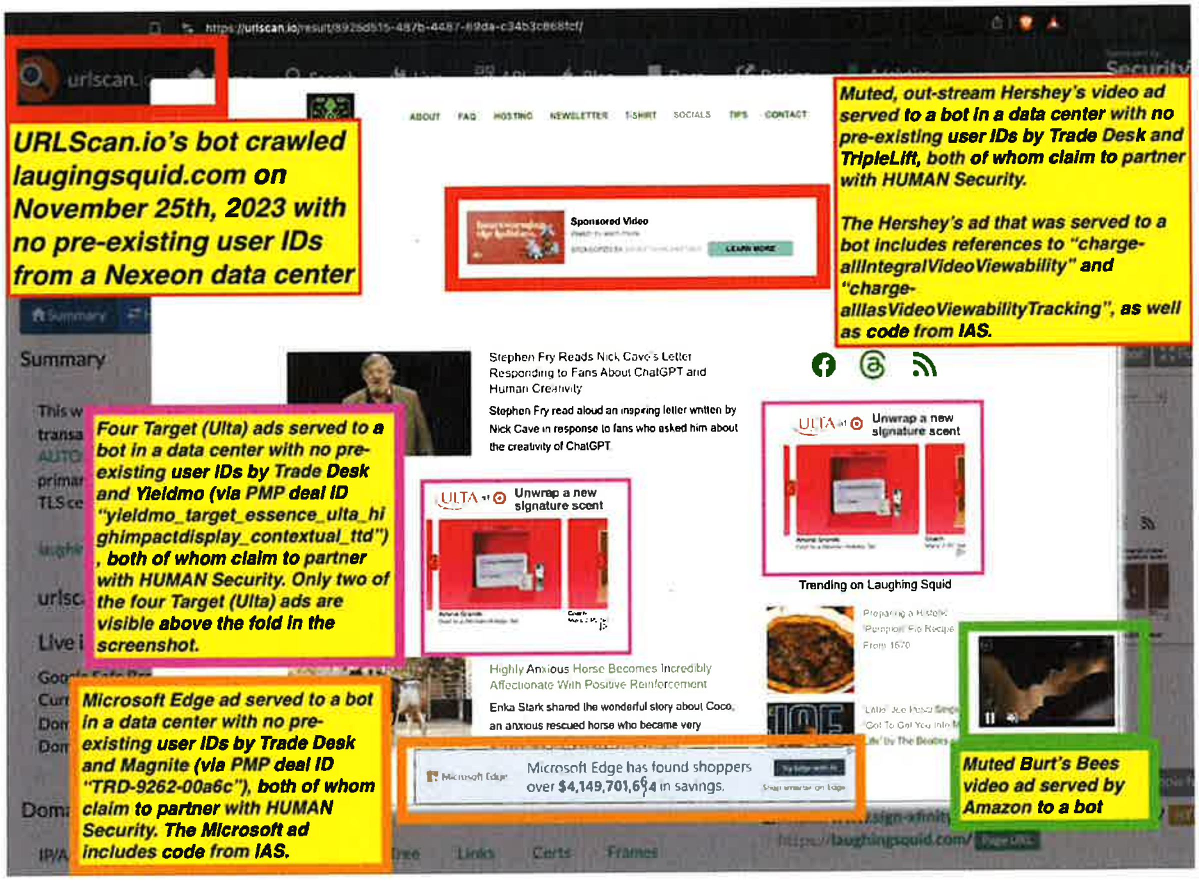
Screenshot of a New York City Police Department (NYPD) ad served to a bot. The ad was served to URLScan.io's bot on June 2, 2023, whilst the bot was crawling applefitnessforum.com. The ad was transacted by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security. Source: https://urlscan.io/result/37d33b15-1345-4637-a664-86897279f57b/

As another example, a Hershey's video ad, four Target Ulta ads (only two of which are visible), a Burt's Bees ad, and a Microsoft edge ad were served to URLScan.io's bot whilst it was crawling laughingsquid.com on November 25th, 2023 with no pre-existing user IDs from a data center.

The Hershey's video ad was transacted by Trade Desk and TripleLift. The source code of the Hershey's ad includes references to IAS, "charge-allIntegralVideoViewability", and "charge-allIasVideoViewabilityTracking".

The four Target (Ulta) ads (of which only two are visible in the screenshot generated by the bot) appear to have been transacted by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_target_essence_ulta_highimpactdisplay_contextual_ttd").

The Microsoft Edge that was served to the bot appears to have been transacted by Trade Desk and Magnite (via PMP deal ID "TRD-9262-00a6c"), both of whom claim to partner with HUMAN Security. The Microsoft ad includes code from IAS.



URLScan.io's bot crawled laugingsquid.com on November 25th, 2023 with no pre-existing user IDs from a Nexeon data center

Muted, out-stream Hershey's video ad served to a bot in a data center with no pre-existing user IDs by Trade Desk and TripleLift, both of whom claim to partner with HUMAN Security.

The Hershey's ad that was served to a bot includes references to "charge-allIntegralVideoViewability" and "charge-allIasVideoViewabilityTracking", as well as code from IAS.

Four Target (Ulta) ads served to a bot in a data center with no pre-existing user IDs by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_target_essence_ulta_highimpactdisplay_contextual_ttd") , both of whom claim to partner with HUMAN Security. Only two of the four Target (Ulta) ads are visible above the fold in the screenshot.

Microsoft Edge ad served to a bot in a data center with no pre-existing user IDs by Trade Desk and Magnite (via PMP deal ID "TRD-9262-00a6c"), both of whom claim to partner with HUMAN Security. The Microsoft ad includes code from IAS.

Muted Burt's Bees video ad served by Amazon to a bot

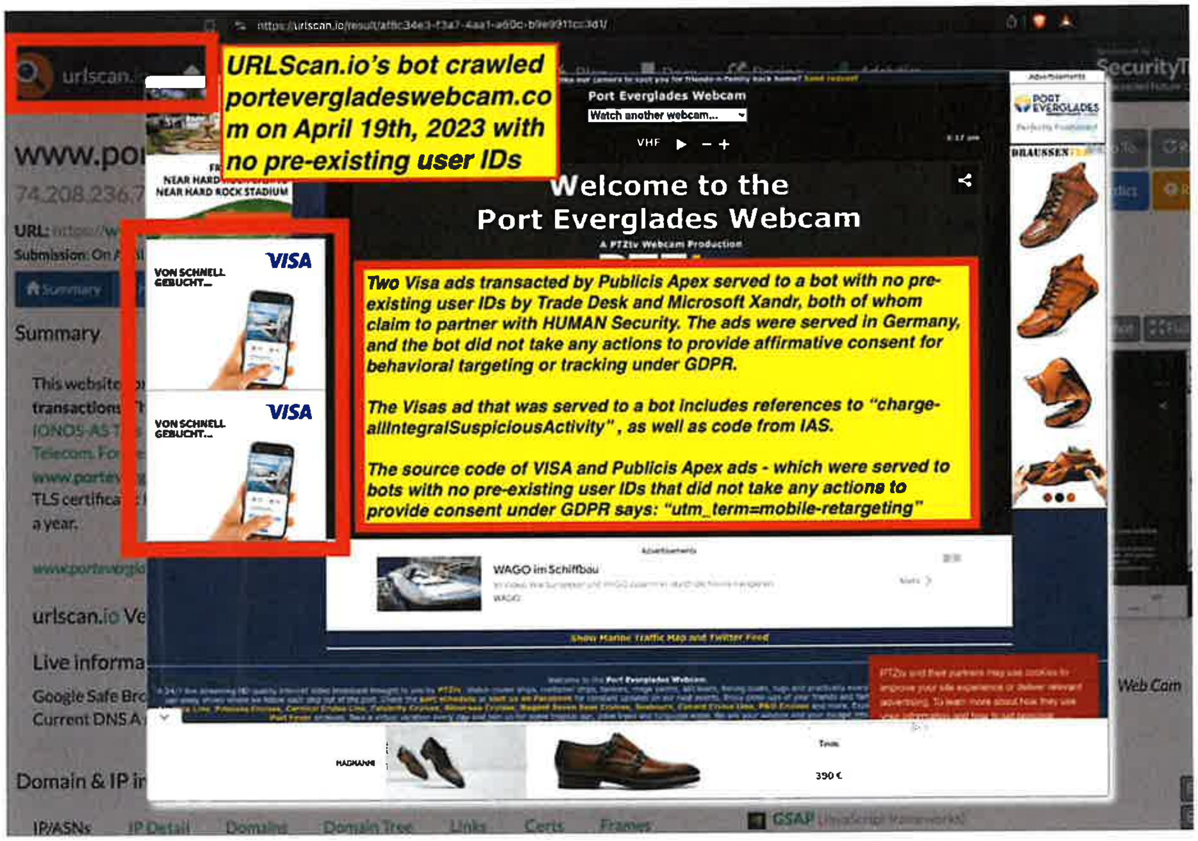
urlscan.io
ABOUT FAQ HOSTING NEWSLETTER T-SHIRT SOCIALS TIPS CONTACT
Sponsored Video
LEARN MORE
Summary
Stephen Fry Reads Nick Cave's Letter Responding to Fans About ChatGPT and Human Creativity
Stephen Fry read aloud an inspiring letter written by Nick Cave in response to fans who asked him about the creativity of ChatGPT
ULTA Unwrap a new signature scent
ULTA Unwrap a new signature scent
Trending on Laughing Squid
Preparing a Historic Pumpkin Pie Recipe From 1670
Highly Anxious Horse Becomes Incredibly Affectionate With Positive Reinforcement
Enka Stark shared the wonderful story about Coco, an anxious rescued horse who became very
Microsoft Edge
Microsoft Edge has found shoppers over $4,149,701,6§4 in savings.
Links Certs Frames
https://laughingsquid.com/

URLScan.io's bot crawled laugingsquid.com on November 25th, 2023 with no pre-existing user IDs from a Nexeon data center. Four Target (Ulta) ads served to a bot in a data center with no pre-existing user IDs *by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_target_essence_ulta_highimpactdisplay_contextual_ttd"), both of whom claim to partner with HUMAN Security. Only two of the four Target (Ulta) ads are visible above the fold in the screenshot. Microsoft Edge ad served to a bot in a data center with no pre-existing user IDs by Trade Desk and Magnite (via PMP deal ID "TRD-9262-00a6c"), both of whom claim to partner with HUMAN Security. The Microsoft ad includes code from IAS. Muted, out-stream Hershey's video ad served to a bot in a data center with no pre-existing user IDs by Trade Desk and TripleLift, both of whom claim to partner with HUMAN Security. The Hershey's ad that was served to a bot includes references to "charge-allIntegralVideoViewability" and "charge-allIasVideoViewabilityTracking", as well as code from IAS.*

https://urlscan.io/result/8926d515-487b-4487-89da-c34b3c868fcf/#summary

As another example, two Visa ads were served to URLScan.io's bot whilst it was crawling portevergladeswebcam.com on April 19th, 2023, from a data center in Germany. The source code of the Visa ads suggest the ads were transacted by Publicis Apex, and were transacted by Trade Desk and Microsoft Xandr SSP, both of whom claim to partner with HUMAN Security. The source code of the Visa ads includes references to "charge-allIntegralSuspiciousActivity" as well as code from IAS.

The URLScan.io bot in Germany did not appear to provide affirmative consent under GDPR for targeted advertising or setting of persistent advertising related identifiers. The source code of the Visa ads says: "utm_term=mobile-retargeting".


URLScan.io's bot crawled portevergladeswebcam.com on April 19th, 2023 with no pre-existing user IDs

Two Visa ads transacted by Publicis Apex served to a bot with no pre-existing user IDs by Trade Desk and Microsoft Xandr, both of whom claim to partner with HUMAN Security. The ads were served in Germany, and the bot did not take any actions to provide affirmative consent for behavioral targeting or tracking under GDPR.

The Visas ad that was served to a bot includes references to "charge-allIntegralSuspiciousActivity", as well as code from IAS.

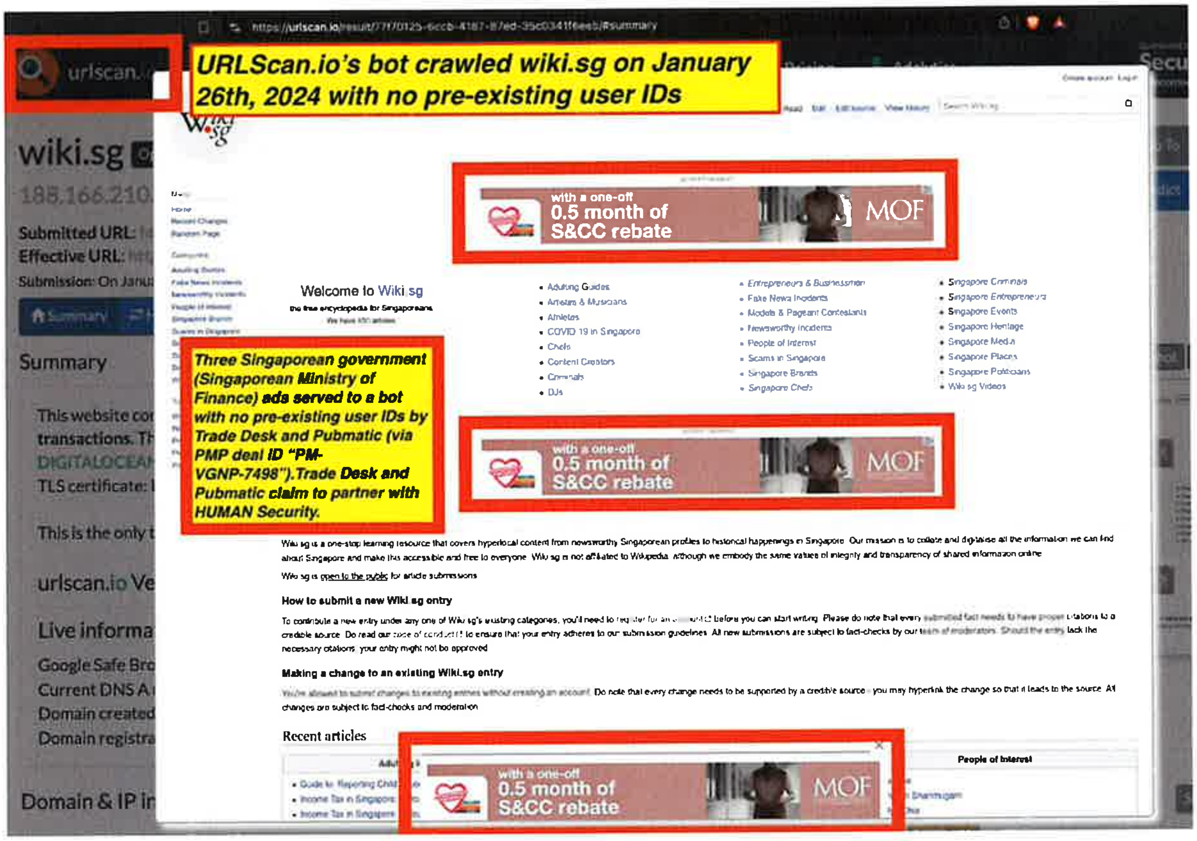
The source code of VISA and Publicis Apex ads - which were served to bots with no pre-existing user IDs that did not take any actions to provide consent under GDPR says: "utm_term=mobile-retargeting"

URLScan.io's bot crawled portevergladeswebcam.com on April 19th, 2023 with no pre-existing user IDs; Two Visa ads transacted by Publicis Apex served to a bot with no pre-existing user IDs by Trade Desk and Microsoft Xandr, both of whom claim to partner with HUMAN Security. The ads were served in Germany, and the bot did not take any actions to provide affirmative consent for behavioral targeting or tracking under GDPR. The Visas ad that was served to a bot includes references to "charge-allIntegralSuspiciousActivity", as well as code from IAS. The source code of VISA and Publicis Apex ads - which were served to bots with no pre-existing user IDs that did not take any actions to provide consent under GDPR says: "utm_term=mobile-retargeting"

Source: https://urlscan.io/result/af8c34e3-f3a7-4aa1-a60c-b9e9911cc3d1/ ; Source: https://urlscan.io/responses/36fd53d0c81ebf9bb5075c7d8987dd967915b191e7cfad3b96a285022e488e25/

As another example, three Singaporean government ads were served to URLScan.io's bot whilst it was crawling wiki.sg on January 26th, 2024.

The Singaporean government ads appear to have been served by Trade Desk and Pubmatic (via PMP deal ID "PM-VGNP-7498"), both of whom claim to partner with HUMAN Security.



URLScan.io's bot crawled wiki.sg on January 26th, 2024 with no pre-existing user IDs

Three Singaporean government (Singaporean Ministry of Finance) ads served to a bot with no pre-existing user IDs by Trade Desk and Pubmatic (via PMP deal ID "PM-VGNP-7498").Trade Desk and Pubmatic claim to partner with HUMAN Security.

Welcome to Wiki.sg

the free encyclopedia for Singaporeans

Wiki.sg is a one-stop learning resource that covers hyperlocal content from newsworthy Singaporean profiles to historical happenings in Singapore. Our mission is to collate and digitalise all the information we can find about Singapore and make this accessible and free to everyone. Wiki.sg is not affiliated to Wikipedia, although we embody the same values of integrity and transparency of shared information online.

Wiki.sg is open to the public for article submissions.

How to submit a new Wiki.sg entry

To contribute a new entry under any one of Wiki.sg's existing categories, you'll need to register for an account before you can start writing. Please do note that every submitted fact needs to have proper citations to a credible source. Do read our code of conduct to ensure that your entry adheres to our submission guidelines. All new submissions are subject to fact-checks by our team of moderators. Should the entry lack the necessary citations, your entry might not be approved.

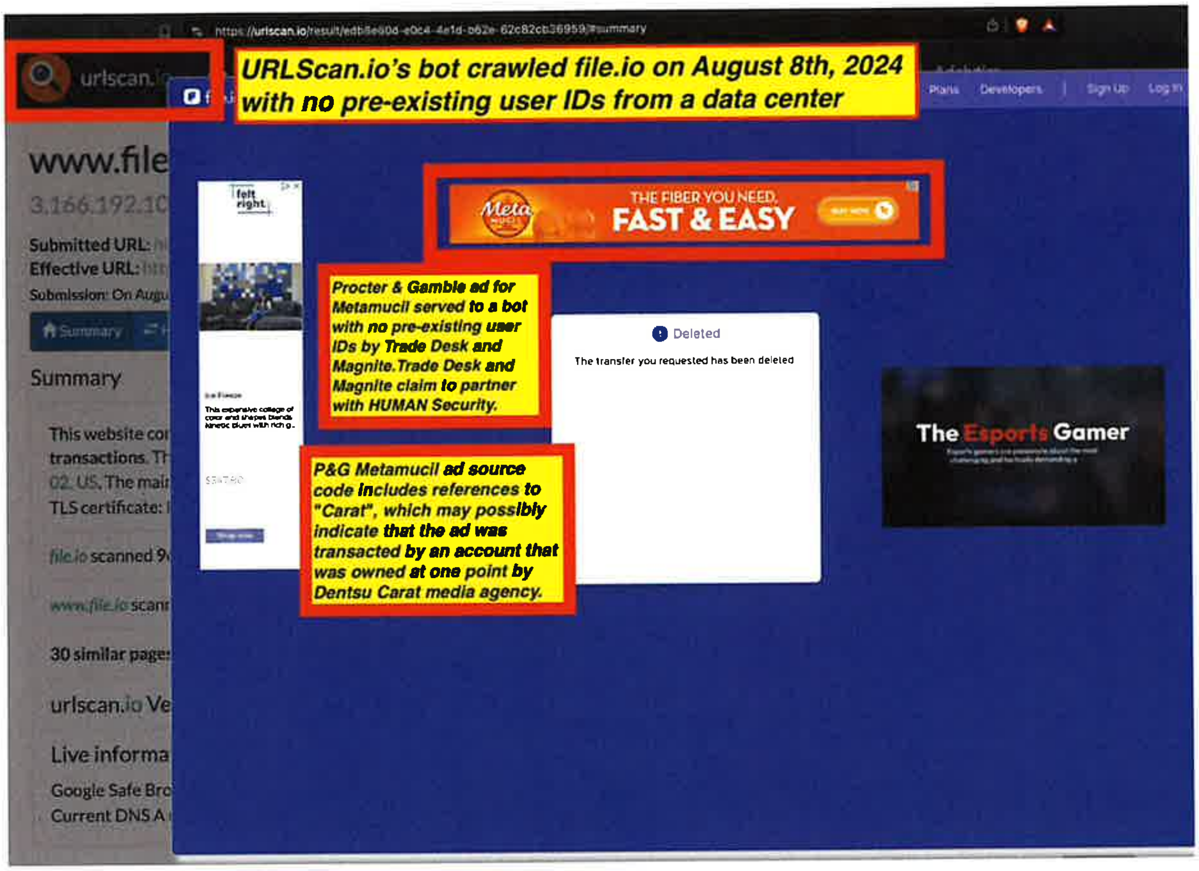
Making a change to an existing Wiki.sg entry

You're allowed to submit changes to existing entries without creating an account. Do note that every change needs to be supported by a credible source - you may hyperlink the change so that it leads to the source. All changes are subject to fact-checks and moderation.

Recent articles

Three Singaporean government ads served to a bot by Trade Desk and Pubmatic. Source: https://urlscan.io/result/77f70125-6ccb-4187-87ed-35c0341f6ee5/

As another example, a Procter & Gamble Metamucil ad was served to URLScan.io's bot whilst it was crawling file.io on August 8th, 2024. The P&G Metamucil ads appear to have been served by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.



URLScan.io's bot crawled file.io on August 8th, 2024 with ***no*** pre-existing user IDs from a data center

Procter & Gamble ad for Metamucil served to a bot with no pre-existing user IDs by Trade Desk and Magnite.Trade Desk and Magnite claim to partner with HUMAN Security.

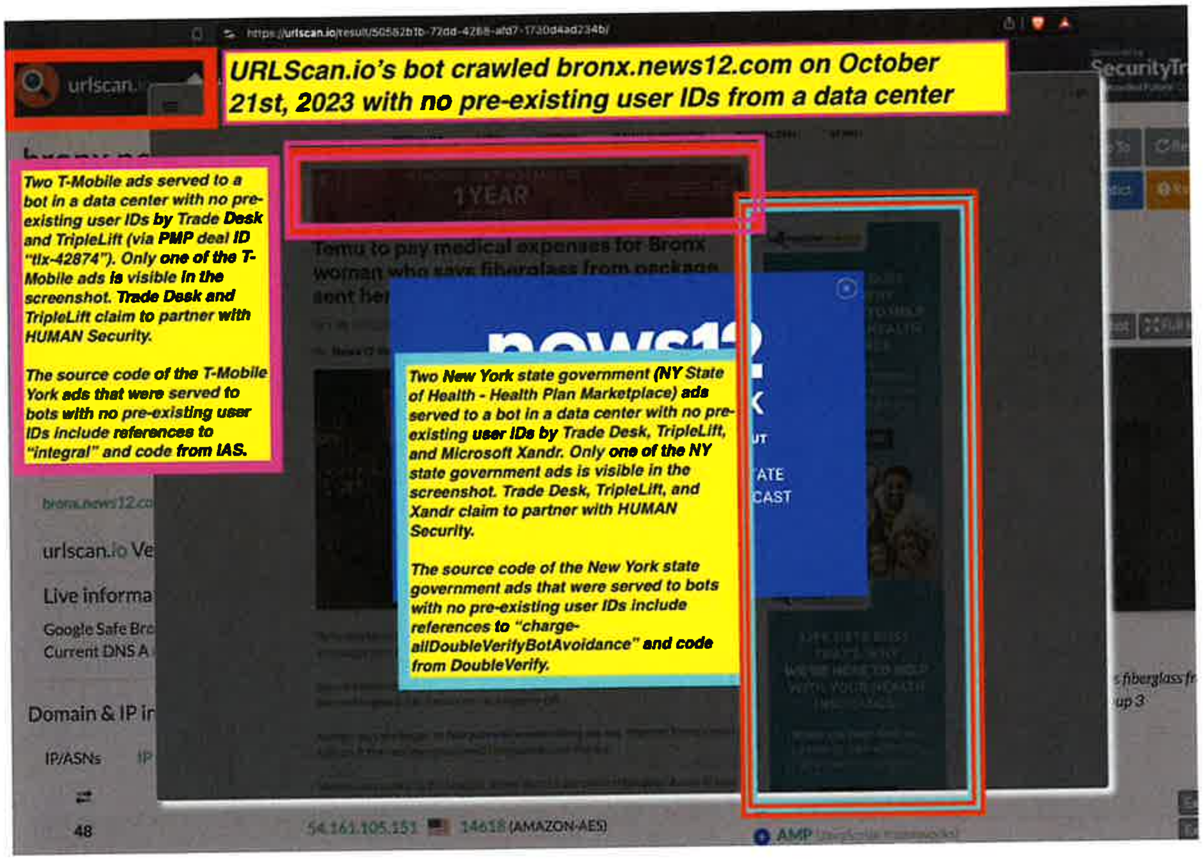
P&G Metamucil ad source code includes references to "Carat", which may possibly indicate that the ad was transacted by an account that was owned at one point by Dentsu Carat media agency.

Deleted

The transfer you requested has been deleted

Source: https://urlscan.io/result/edb8e60d-e0c4-4e1d-b62e-62c82cb36959/

As another example, two New York state government ads and two T-Mobile ads were served to URLScan.io's bot whilst it was crawling bronx.news12.com on October 21st, 2023. The New York state government ads were transacted by Trade Desk, Triplelift and Microsoft Xandr SSP, all three of whom claim to partner with HUMAN Security. The source code of the New York state government ads includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. The two T-Mobile ads appear to have been served by Trade Desk and Triplelift (via PMP deal ID "tlx-42874"). The T-Mobile ads include code from IAS.


https://urlscan.io/result/50582b1b-72dd-4288-afd7-1730d4ad234b/
urlscan.io
1 YEAR
Temu to pay medical expenses for Bronx woman who says fiberglass from package sent her
news12
bronx.news12.com
urlscan.io Ve
Live informa
Google Safe Bro
Current DNS A
Domain & IP ir
IP/ASNs
48
54.161.105.151 14618 (AMAZON-AES)
AMP
SecurityTr

URLScan.io's bot crawled bronx.news12.com on October 21st, 2023 with no pre-existing user IDs from a data center

Two T-Mobile ads served to a bot in a data center with no pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-42874"). Only one of the T-Mobile ads is visible in the screenshot. Trade Desk and TripleLift claim to partner with HUMAN Security.

The source code of the T-Mobile York ads that were served to bots with no pre-existing user IDs include references to "integral" and code from IAS.

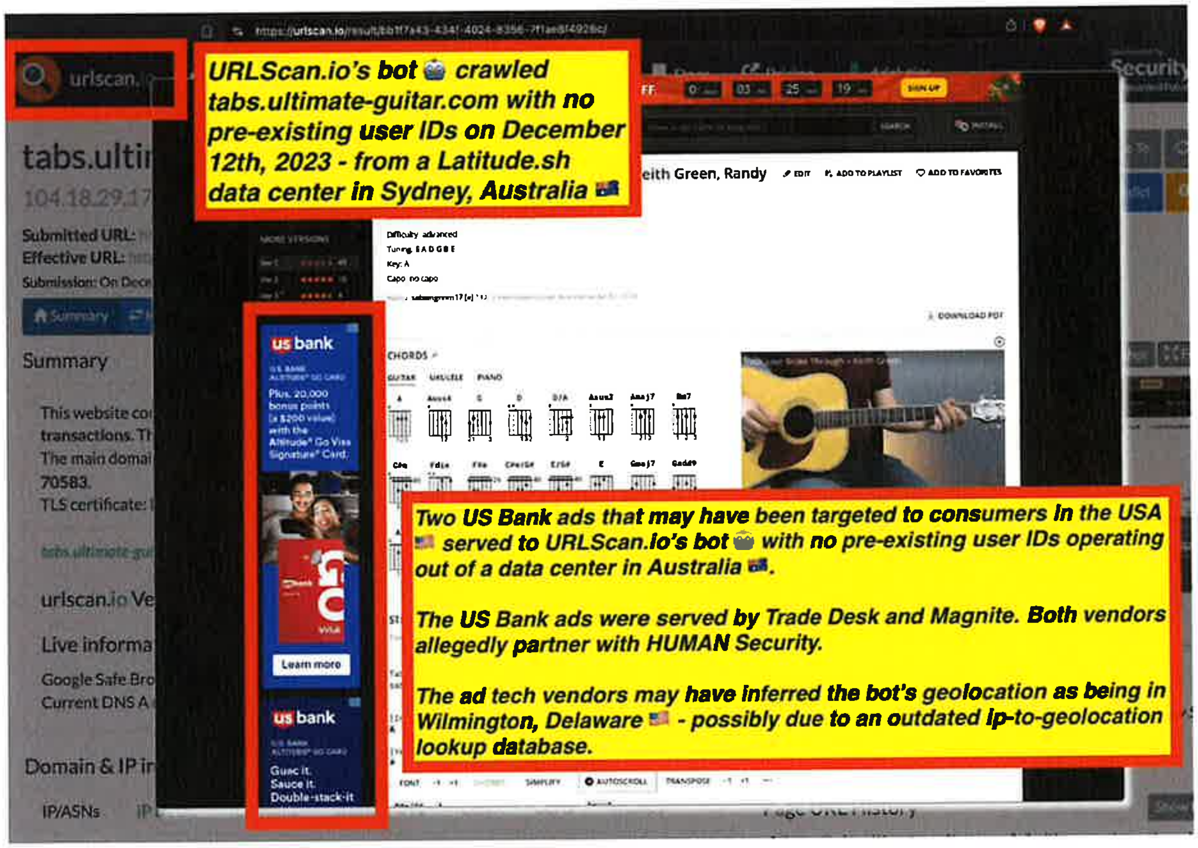
Two New York state government (NY State of Health - Health Plan Marketplace) ads served to a bot in a data center with no pre-existing user IDs by Trade Desk, TripleLift, and Microsoft Xandr. Only one of the NY state government ads is visible in the screenshot. Trade Desk, TripleLift, and Xandr claim to partner with HUMAN Security.

The source code of the New York state government ads that were served to bots with no pre-existing user IDs include references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

Two New York state government ads and two T-Mobile ads served to URLScan.io's bot by Trade Desk, Triplelift, and Xandr. The New York state government ads include references to "charge-allDoubleVerifyBotAvoidance". Source: https://urlscan.io/result/50582b1b-72dd-4288-afd7-1730d4ad234b/

As another example, two US Bank ads were served to URLScan.io's bot whilst it was crawling tabs.ultimate-guitar.com on December 12th, 2023 from a data center in Australia. The two US Bank ads were transacted by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.

The US Bank ads appear to have been targeted to a consumer in Wilmington, Delaware, USA but were served to a bot in a data center in Australia. This may potentially be due to the ad tech vendors using an out-dated ip-to-geolocation lookup table.



URLScan.io's bot 🤖 crawled tabs.ultimate-guitar.com with no pre-existing user IDs on December 12th, 2023 - from a Latitude.sh data center in Sydney, Australia 🇦🇺

Two US Bank ads that may have been targeted to consumers in the USA 🇺🇸 served to URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.

The US Bank ads were served by Trade Desk and Magnite. Both vendors allegedly partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Wilmington, Delaware 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

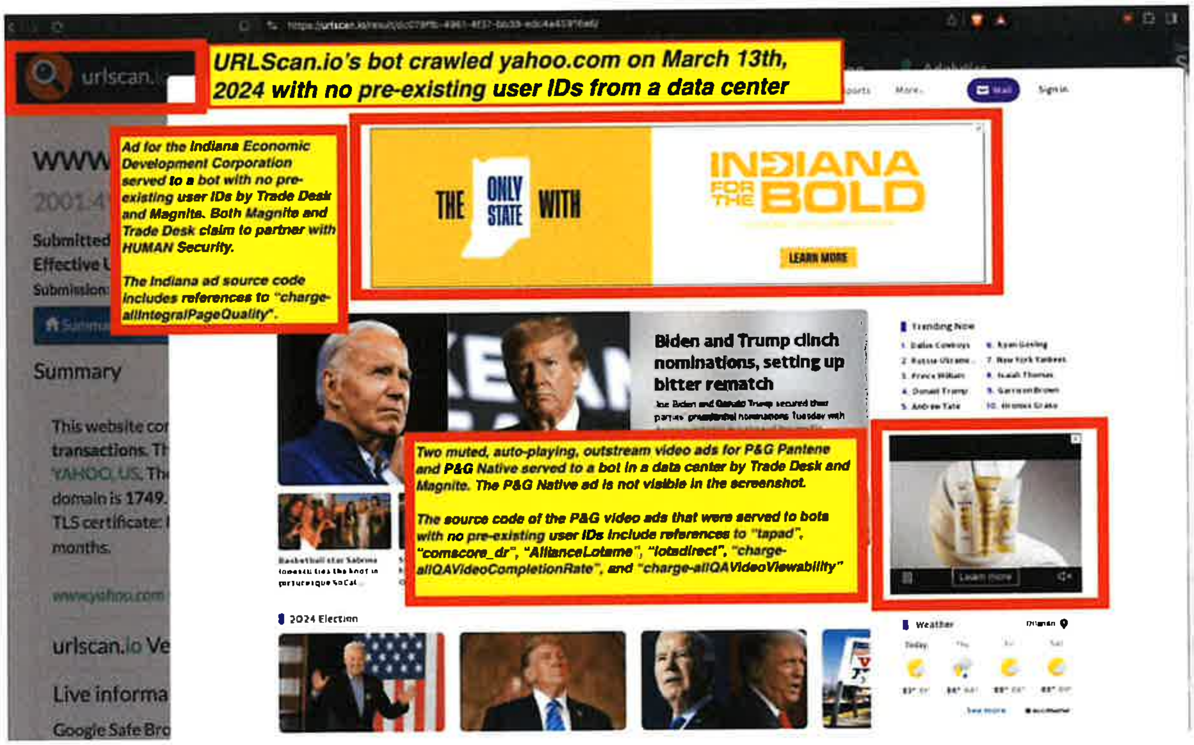
URLScan.io's bot 🤖 crawled tabs.ultimate-guitar.com with no pre-existing user IDs on December 12th, 2023 - from a Latitude.sh data center in Sydney, Australia AU. Two US Bank ads that may have been targeted to consumers in the USA US served to URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia AU. The US Bank ads were served by Trade Desk and Magnite. Both vendors allegedly partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Wilmington, Delaware US - possibly due to an outdated ip-to-geolocation lookup database.

Source: https://urlscan.io/result/bb1f7a43-434f-4024-8356-7f1ae8f4926c/

As another example, an Indiana state government ad, a Procter & Gamble Pantene video ad, and a P&G Native deodorant ad were served to URLScan.io's bot whilst it was crawling yahoo.com on March 13th, 2024. The Indiana state government ad was served by Trade Desk and

Magnite, and includes references to IAS and "charge-allIntegralPageQuality."

The two muted, auto-playing out-stream P&G ads were transacted by Trade Desk and Magnite, and include references to "charge-allQAVideoViewability", "tapad", "comscore_dr", "alliancelotame", "lotadirect", and "charge-allVideoCompletionRate".



URLScan.io's bot crawled yahoo.com on March 13th, 2024 with no pre-existing user IDs from a data center

Ad for the Indiana Economic Development Corporation served to a bot with no pre-existing user IDs by Trade Desk and Magnite. Both Magnite and Trade Desk claim to partner with HUMAN Security.

The Indiana ad source code includes references to "charge-allIntegralPageQuality".

Two muted, auto-playing, outstream video ads for P&G Pantene and P&G Native served to a bot in a data center by Trade Desk and Magnite. The P&G Native ad is not visible in the screenshot.

The source code of the P&G video ads that were served to bots with no pre-existing user IDs include references to "tapad", "comscore_dr", "AllianceLotame", "lotadirect", "charge-allQAVideoCompletionRate", and "charge-allQAVideoViewability"

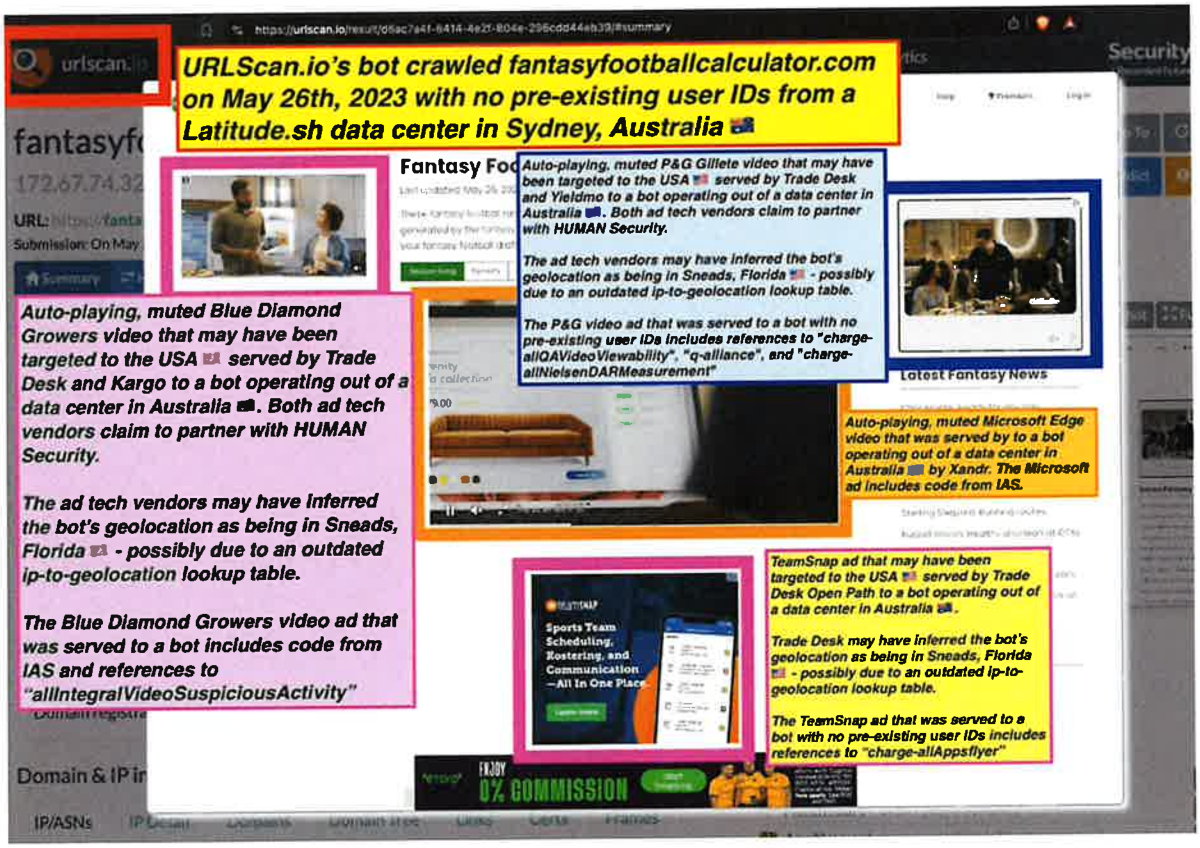
Indiana state government and two P&G muted, auto-playing, outstream video ads served to a bot with no pre-existing user identifiers. Source: https://urlscan.io/result/dc079ffb-4961-4f37-bb38-edc4a45916a6/

As another example, a Blue Diamond Growers video ad, P&G Gillette video ad, Microsoft Edge video ad, and TeamSnap ad were served to URLScan.io's bot whilst the bot was crawling fantasyfootballcalculator.com on May 26th, 2023 from a data center in Australia.

The Blue Diamond, P&G Gillette, and TeamSnap ads were transacted by Trade Desk DSP and by Kargo, Yieldmo, and Trade Desk Open Path (respectively). The ads appear to have been targeted to a consumer in

Sneads, Florida but were served to a bot with no user identifiers in a data center in Australia, possibly due to one or more ad tech vendors using an out-dated IP address to geolocation lookup table.

The muted, auto-playing, outstream Blue Diamond Growers video ad includes code from IAS and references to “charge-allIntegralVideoSuspiciousActivity”. The muted, auto-playing, out-stream P&G Gillette video ad that was served to a bot with no pre-existing user identifiers includes references to “charge-allQAVideoViewability”, “q-alliance”, and “charge-allNielsenDARMeasurement”. The TeamSnap ad includes references to “charge-allAppsflyer”.



URLScan.io's bot crawled fantasyfootballcalculator.com on May 26th, 2023 with no pre-existing user IDs from a Latitude.sh data center in Sydney, Australia

Auto-playing, muted P&G Gillete video that may have been targeted to the USA served by Trade Desk and Yieldmo to a bot operating out of a data center in Australia. Both ad tech vendors claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Sneads, Florida - possibly due to an outdated ip-to-geolocation lookup table.

The P&G video ad that was served to a bot with no pre-existing user IDs includes references to "charge-allQAVideoViewability", "q-alliance", and "charge-allNielsenDARMeasurement"

Auto-playing, muted Blue Diamond Growers video that may have been targeted to the USA served by Trade Desk and Kargo to a bot operating out of a data center in Australia. Both ad tech vendors claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Sneads, Florida - possibly due to an outdated ip-to-geolocation lookup table.

The Blue Diamond Growers video ad that was served to a bot includes code from IAS and references to "allIntegralVideoSuspiciousActivity"

Auto-playing, muted Microsoft Edge video that was served by to a bot operating out of a data center in Australia by Xandr. The Microsoft ad includes code from IAS.

TeamSnap ad that may have been targeted to the USA served by Trade Desk Open Path to a bot operating out of a data center in Australia.

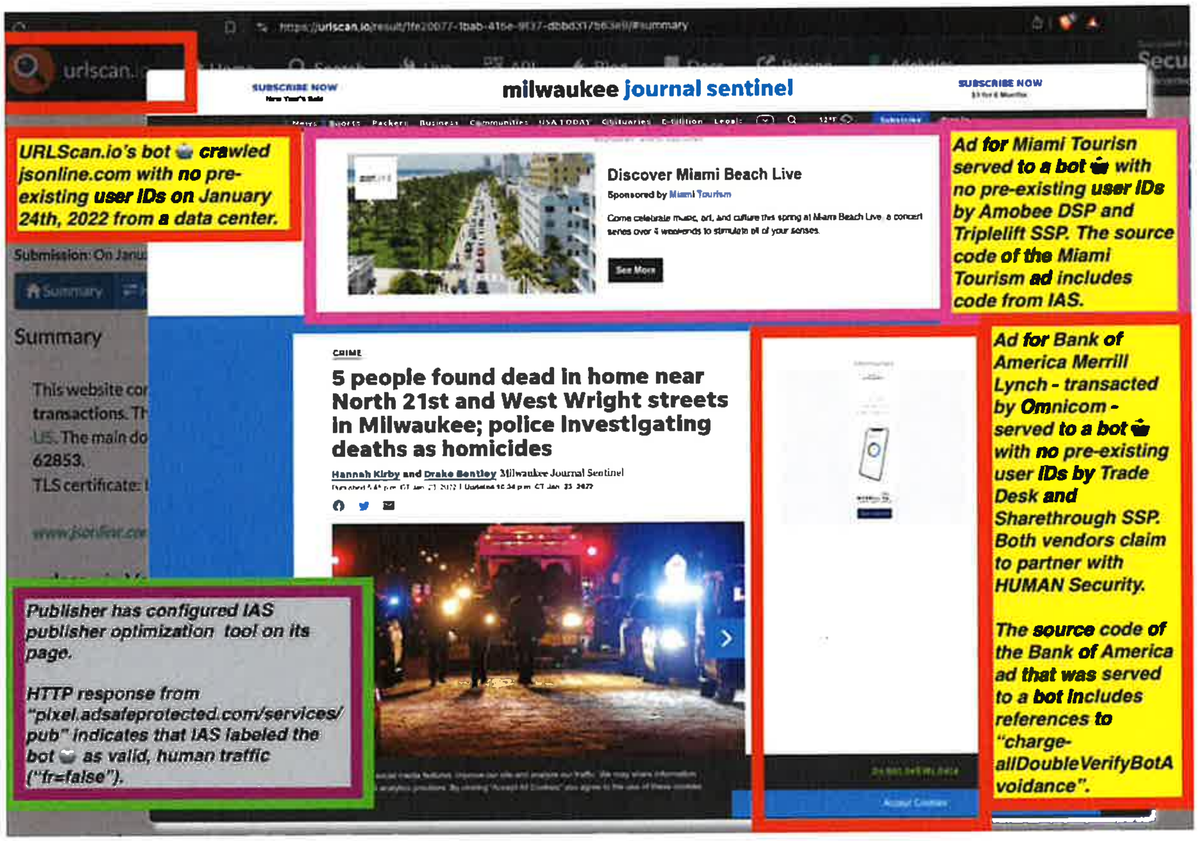
Trade Desk may have inferred the bot's geolocation as being in Sneads, Florida - possibly due to an outdated ip-to-geolocation lookup table.

The TeamSnap ad that was served to a bot with no pre-existing user IDs includes references to "charge-allAppsflyer"

A Blue Diamond Growers, a P&G Gillette, and a TeamSnap ad served to a bot in a data center in Australia with no pre-existing user identifiers. The source code of the Blue Diamond Growers ad includes references to “charge-allIntegralVideoSuspiciousActivity”. Source: https://urlscan.io/result/d6ac7a4f-6414-4e2f-804e-296cdd44eb39/

As another example, a Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling jsonline.com on January 24th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Sharethrough, all three of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".

The publisher jsonline.com appears to have configured IAS' publisher optimization tool on its page. The IAS tool appears to have classified the URLScan.io bot as "fr=false" (valid, human traffic).



URLScan.io's bot 🤖 crawled jsonline.com with no pre-existing user IDs on January 24th, 2022 from a data center.

Ad for Miami Tourism served to a bot 🤖 with no pre-existing user IDs by Amobee DSP and Triplelift SSP. The source code of the Miami Tourism ad includes code from IAS.

5 people found dead in home near North 21st and West Wright streets in Milwaukee; police investigating deaths as homicides

Hannah Kirby and Drake Bentley Milwaukee Journal Sentinel

Ad for Bank of America Merrill Lynch - transacted by Omnicom - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Sharethrough SSP. Both vendors claim to partner with HUMAN Security.

The source code of the Bank of America ad that was served to a bot includes references to "charge-allDoubleVerifyBotAvoidance".

Publisher has configured IAS publisher optimization tool on its page.

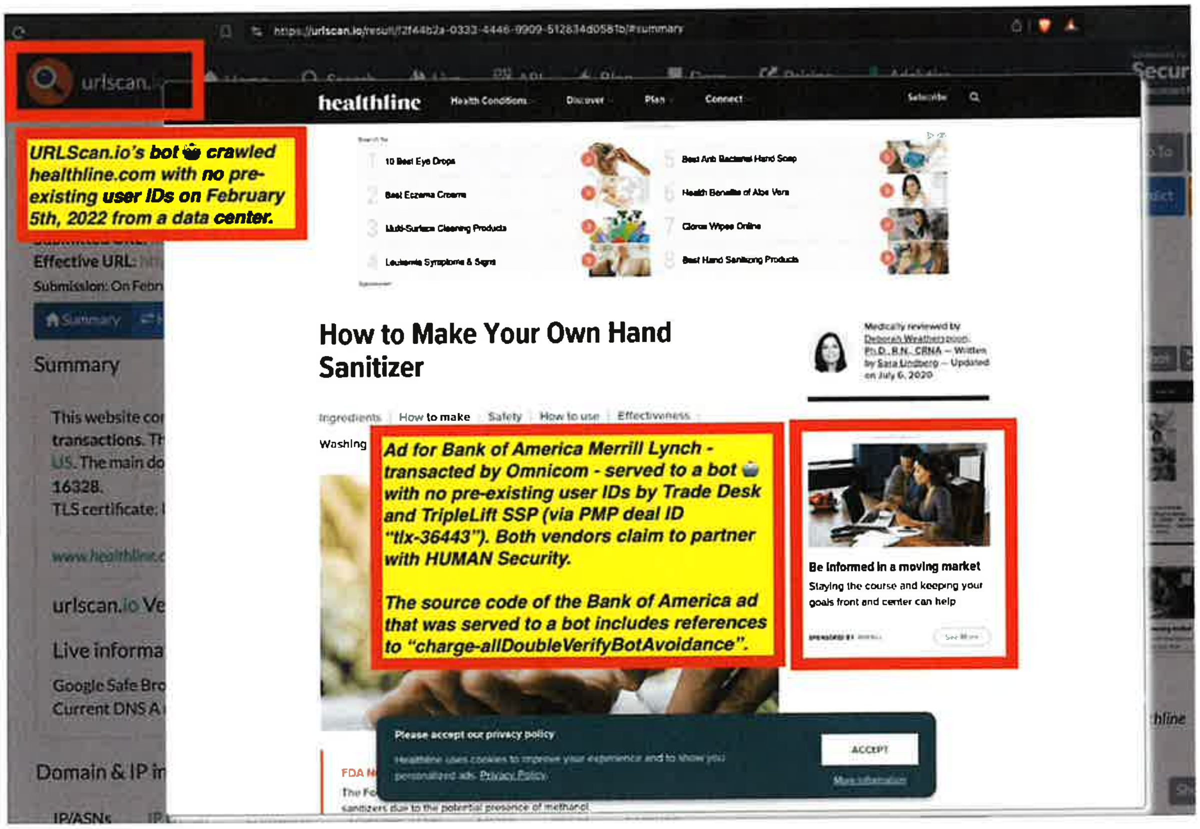
HTTP response from "pixel.adsafeprotected.com/services/pub" indicates that IAS labeled the bot 🤖 as valid, human traffic ("fr=false").

Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling jsonline.com on January 24th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Sharethrough, both of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Source: https://urlscan.io/result/1fe20077-1bab-415e-9f37-dbbd317563e9/

As another example, a Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling healthline.com on February 5th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Triplelift (via PMP deal ID "tlx-36443"), all three of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".



https://urlscan.io/result/f2f44b2a-0333-4446-8909-512834d0581b/#summary

URLScan.io's bot 🤖 crawled healthline.com with no pre-existing user IDs on February 5th, 2022 from a data center.

How to Make Your Own Hand Sanitizer

Medically reviewed by Deborah Weatherspoon, Ph.D., R.N., CRNA — Written by Sara Lindberg — Updated on July 6, 2020

Ad for Bank of America Merrill Lynch - transacted by Omnicom - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and TripleLift SSP (via PMP deal ID "tlx-36443"). Both vendors claim to partner with HUMAN Security.

The source code of the Bank of America ad that was served to a bot includes references to "charge-allDoubleVerifyBotAvoidance".

Be informed in a moving market

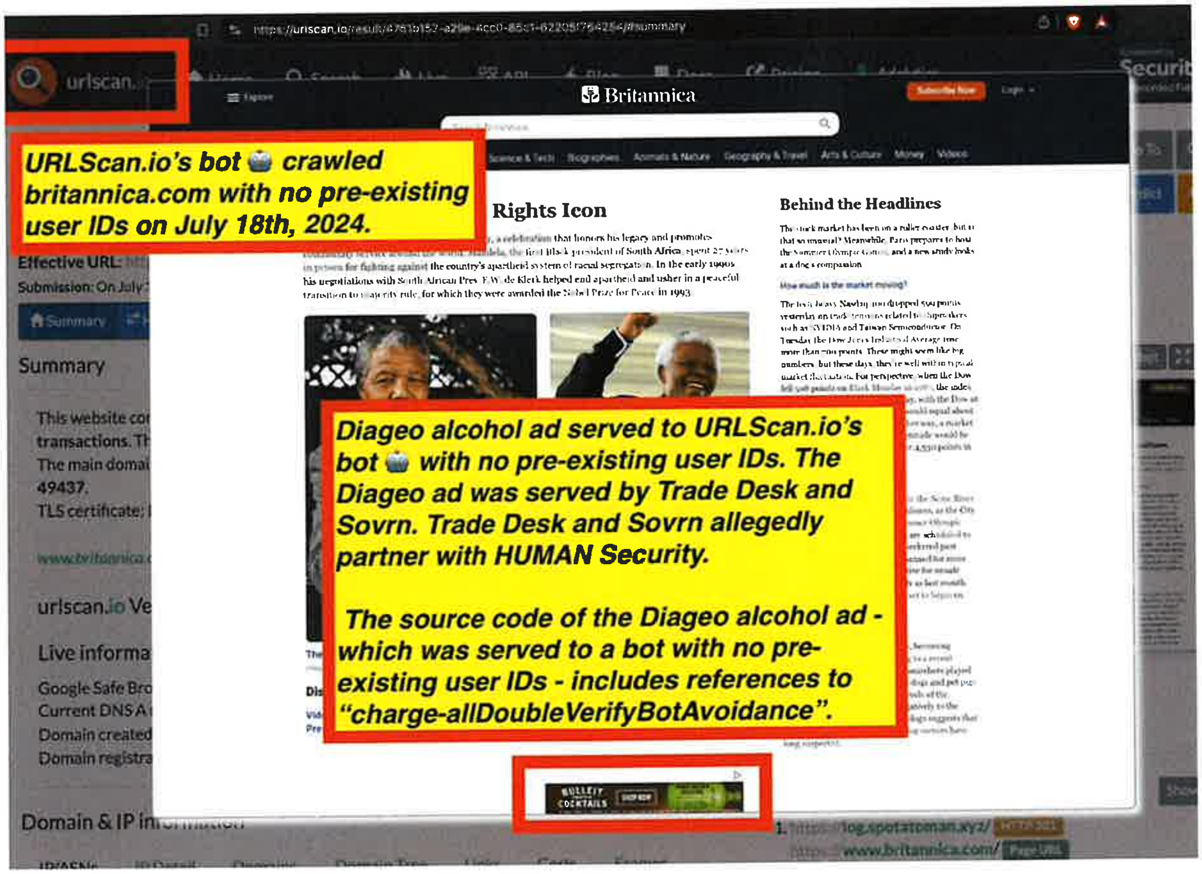
Staying the course and keeping your goals front and center can help

Healthline uses cookies to improve your experience and to show you personalized ads. Privacy Policy.

Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling healthline.com on February 5th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Triplelift, both of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".

Source: https://urlscan.io/result/f2f44b2a-0333-4446-9909-512834d0581b/

As another example, a Diageo alcohol ad was served to URLScan.io's bot whilst the bot was crawling britannica.com on July 18th, 2024. The Diageo ad appears to have been served by Trade Desk and Sovrn, both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".



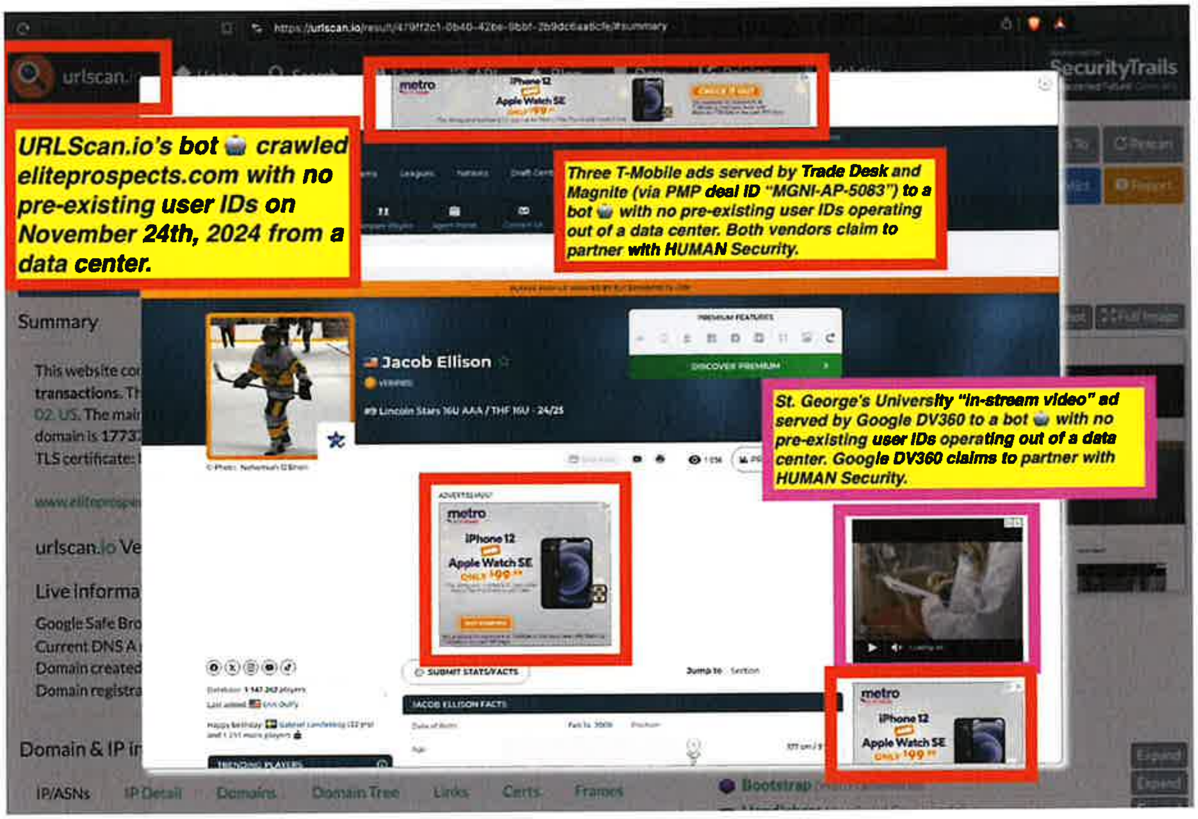
URLScan.io's bot 🤖 crawled britannica.com with no pre-existing user IDs on July 18th, 2024.

Diageo alcohol ad served to URLScan.io's bot 🤖 with no pre-existing user IDs. The Diageo ad was served by Trade Desk and Sovrn. Trade Desk and Sovrn allegedly partner with HUMAN Security.

The source code of the Diageo alcohol ad - which was served to a bot with no pre-existing user IDs - includes references to "charge-allDoubleVerifyBotAvoidance".

Diageo alcohol ad was served to URLScan.io's bot whilst the bot was crawling britannica.com on July 18th, 2024. The Diageo ad appears to have been served by Trade Desk and Sovrn, both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance". Source: https://urlscan.io/result/4761b152-a29e-4cc0-85c1-62205f764254/

As another example, three T-Mobile ads and a St George's University ad were served to URLScan.io's bot whilst the bot was crawling eliteprospects.com on November 24th, 2024. The three T-Mobile ads appear to have been transacted by Trade Desk and Magnite (via PMP deal ID "MGNI-AP-5083"), both of whom claim to partner with HUMAN Security. The St. George's University video ad appears to have been served by Google DV360.



URLScan.io's bot 🤖 crawled eliteprospects.com with no pre-existing user IDs on November 24th, 2024 from a data center.

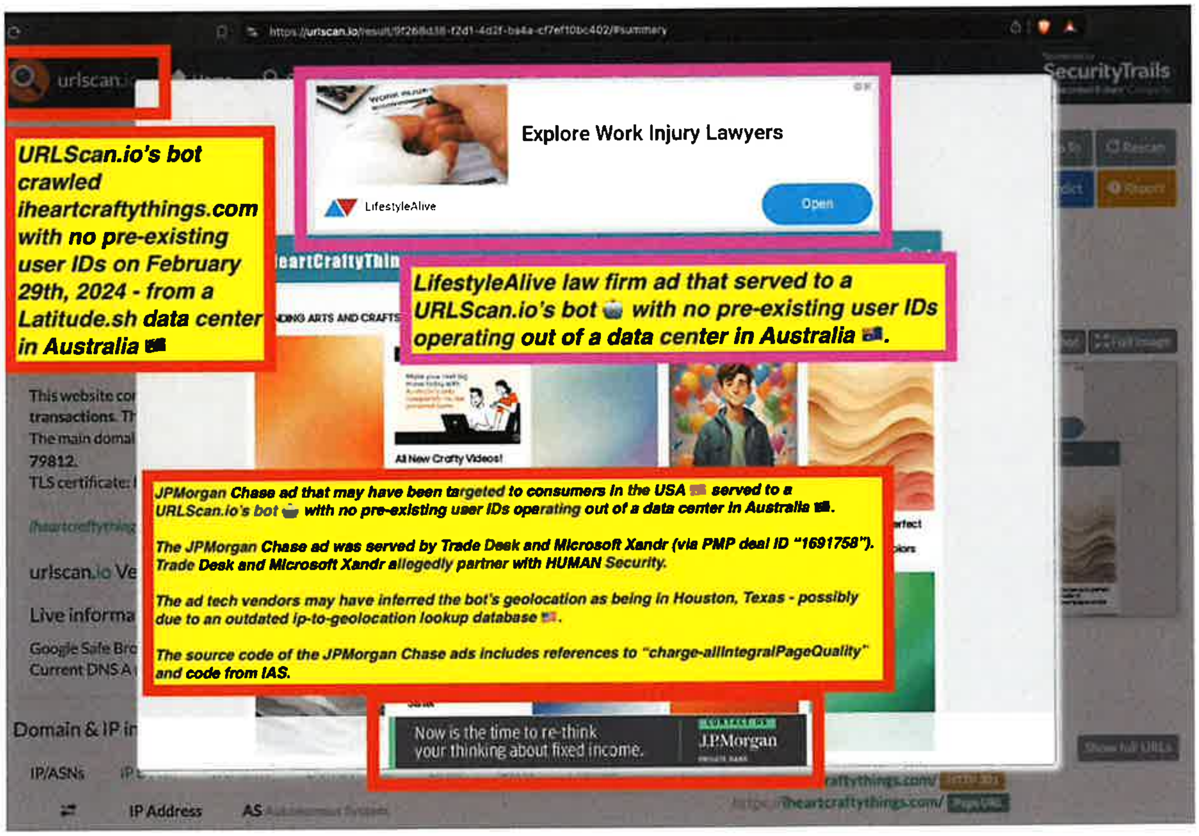
Three T-Mobile ads served by Trade Desk and Magnite (via PMP deal ID "MGNI-AP-5083") to a bot 🤖 with no pre-existing user IDs operating out of a data center. Both vendors claim to partner with HUMAN Security.

St. George's University "in-stream video" ad served by Google DV360 to a bot 🤖 with no pre-existing user IDs operating out of a data center. Google DV360 claims to partner with HUMAN Security.

Three T-Mobile ads and a St George's University ad were served to URLScan.io's bot whilst the bot was crawling eliteprospects.com on November 24th, 2024. The three T-Mobile ads appear to have been transacted by Trade Dek and Magnite (via PMP deal ID "MGNI-AP-5083"), both of whom claim to partner with HUMAN Security. The St. George's University video ad appears to have been served by Google DV360. Source: https://urlscan.io/result/479ff2c1-0b40-42be-9bbf-2b9dc6aa6cfe/#summary

As another example, a JPMorgan Chase ad and a LifeStyleAlive law firm ad was served to URLScan.io's bot whilst the bot was crawling iheartcraftythings.com on February 29th, 2024 from a data center in Australia. The JPMorgan Chase ad appears to have been served by Trade Desk and Microsoft Xandr SSP (via PMP deal ID "1691758"), both of whom claim to partner with HUMAN Security. The source code of the JPMorgan Chase ad includes code from IAS and references to "charge-allIntegralPageQuality".

The JPMorgan Chase ad appears to have been targeted to a consumer in Houston, Texas when it was served to a bot in a data center in Australia. It is possible that one or more ad tech vendors are using an out-dated IP address to geolocation lookup table.



URLScan.io's bot crawled iheartcraftythings.com with no pre-existing user IDs on February 29th, 2024 - from a Latitude.sh data center in Australia 🇦🇺

LifestyleAlive law firm ad that served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.

JPMorgan Chase ad that may have been targeted to consumers in the USA 🇺🇸 served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.

The JPMorgan Chase ad was served by Trade Desk and Microsoft Xandr (via PMP deal ID "1691758"). Trade Desk and Microsoft Xandr allegedly partner with HUMAN Security.

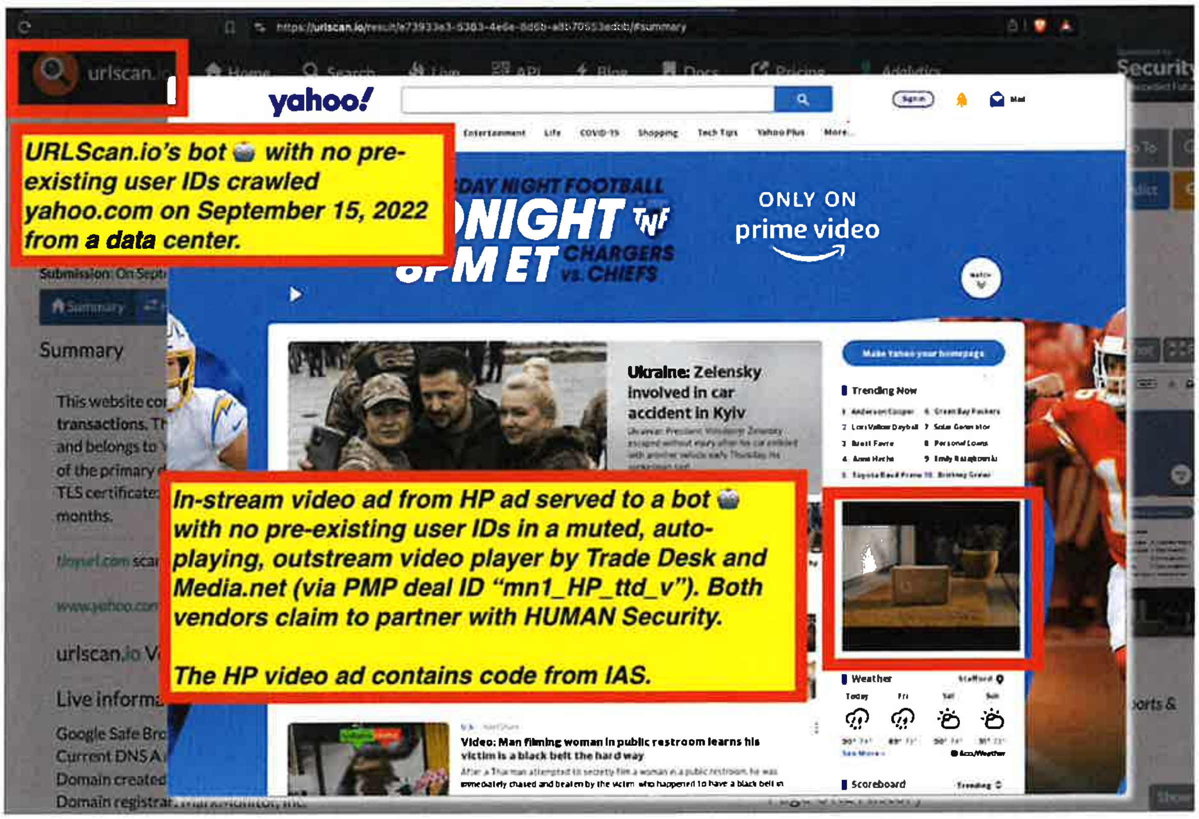
The ad tech vendors may have inferred the bot's geolocation as being in Houston, Texas - possibly due to an outdated ip-to-geolocation lookup database 🇺🇸.

The source code of the JPMorgan Chase ads includes references to "charge-allIntegralPageQuality" and code from IAS.

URLScan.io's bot crawled iheartcraftythings.com with no pre-existing user IDs on February 29th, 2024 - from a Latitude.sh data center in Australia AU. JPMorgan Chase ad that may have been targeted to consumers in the USA US served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia AU. The JPMorgan Chase ad was served by Trade Desk and Microsoft Xandr (via PMP deal ID "1691758"). Trade Desk and Microsoft Xandr allegedly *partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Houston, Texas - possibly due to an outdated ip-to-geolocation lookup database US. The source code of the JPMorgan Chase ads includes references to "charge-allIntegralPageQuality" and code from IAS. LifestyleAlive law firm ad that served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia AU.*

Source: https://urlscan.io/result/9f268d38-f2d1-4d2f-ba4a-cf7ef10bc402/#summary

As another example, a muted, auto-playing, outstream HP video ad was served to URLScan.io's bot whilst the bot was crawling yahoo.com on September 15th, 2022. The HP video ad appears to have been served by Trade Desk and Media.net (via PMP deal ID "mn1_HP_ttd_v"), both of whom claim to partner with HUMAN Security, The HP ad includes code from IAS.



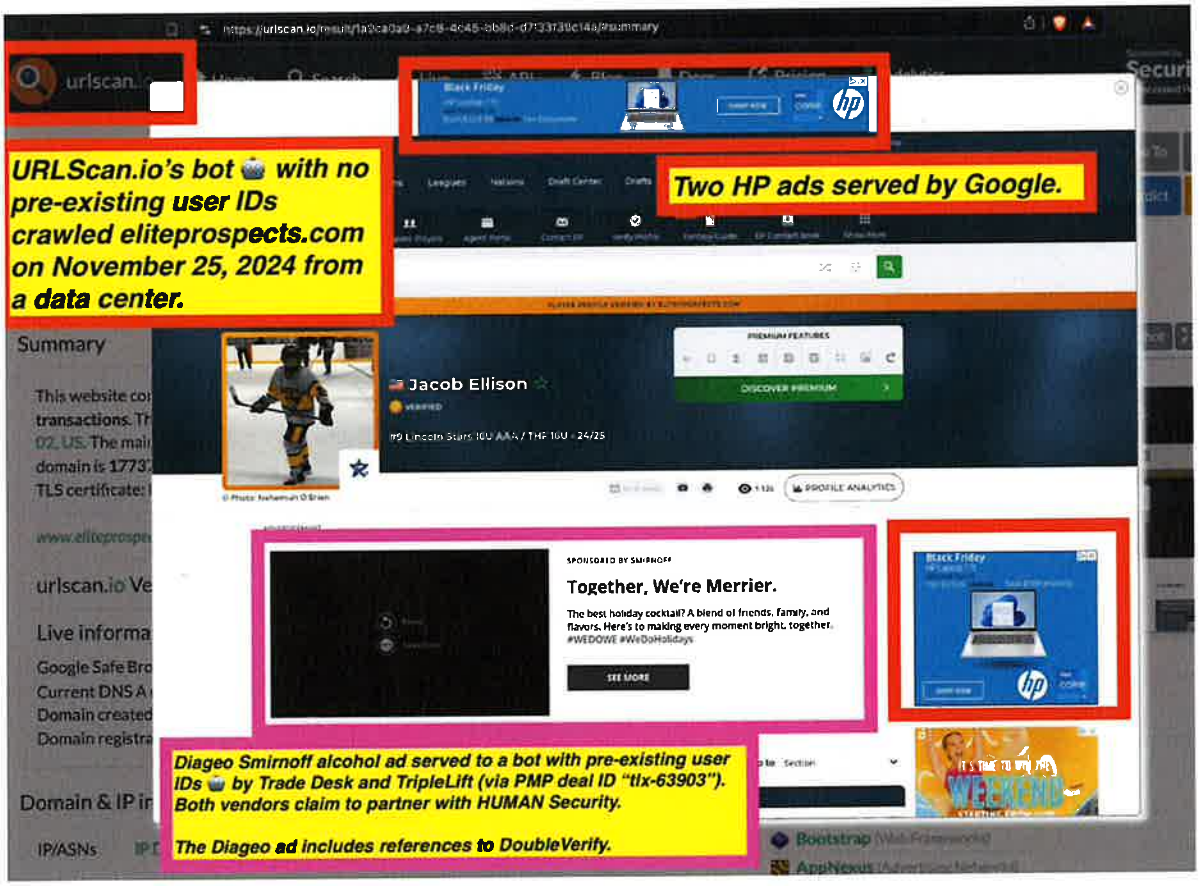
URLScan.io's bot 🤖 with no pre-existing user IDs crawled yahoo.com on September 15, 2022 from a data center.

In-stream video ad from HP ad served to a bot 🤖 with no pre-existing user IDs in a muted, auto-playing, outstream video player by Trade Desk and Media.net (via PMP deal ID "mn1_HP_ttd_v"). Both vendors claim to partner with HUMAN Security.

The HP video ad contains code from IAS.

A muted, auto-playing, outstream HP video ad was served to URLScan.io's bot whilst the bot was crawling yahoo.com on September 15th, 2022. The HP video ad appears to have been served by Trade Desk and Media.net (via PMP deal ID "mn1_HP_ttd_v"), both of whom claim to partner with HUMAN Security, The HP ad includes code from IAS. Source: https://urlscan.io/result/e73933e3-5383-4e6e-8d6b-a8b70553edbb/

As another example, a Diageo Smirnoff alcohol ad was served to URLScan.io's bot whilst the bot was crawling eliteprospects.com on November 25th, 2024 with no pre-existing user identifiers. The Diageo alcohol ad appears to have been served by Trade Desk and Triplelift (via PMP deal ID "tlx-63903"), both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance". Two HP ads were also served to the bot with no pre-existing user identifiers.



URLScan.io's bot with no pre-existing user IDs crawled eliteprospects.com on November 25, 2024 from a data center.

Two HP ads served by Google.

Diageo Smirnoff alcohol ad served to a bot with pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-63903"). Both vendors claim to partner with HUMAN Security.

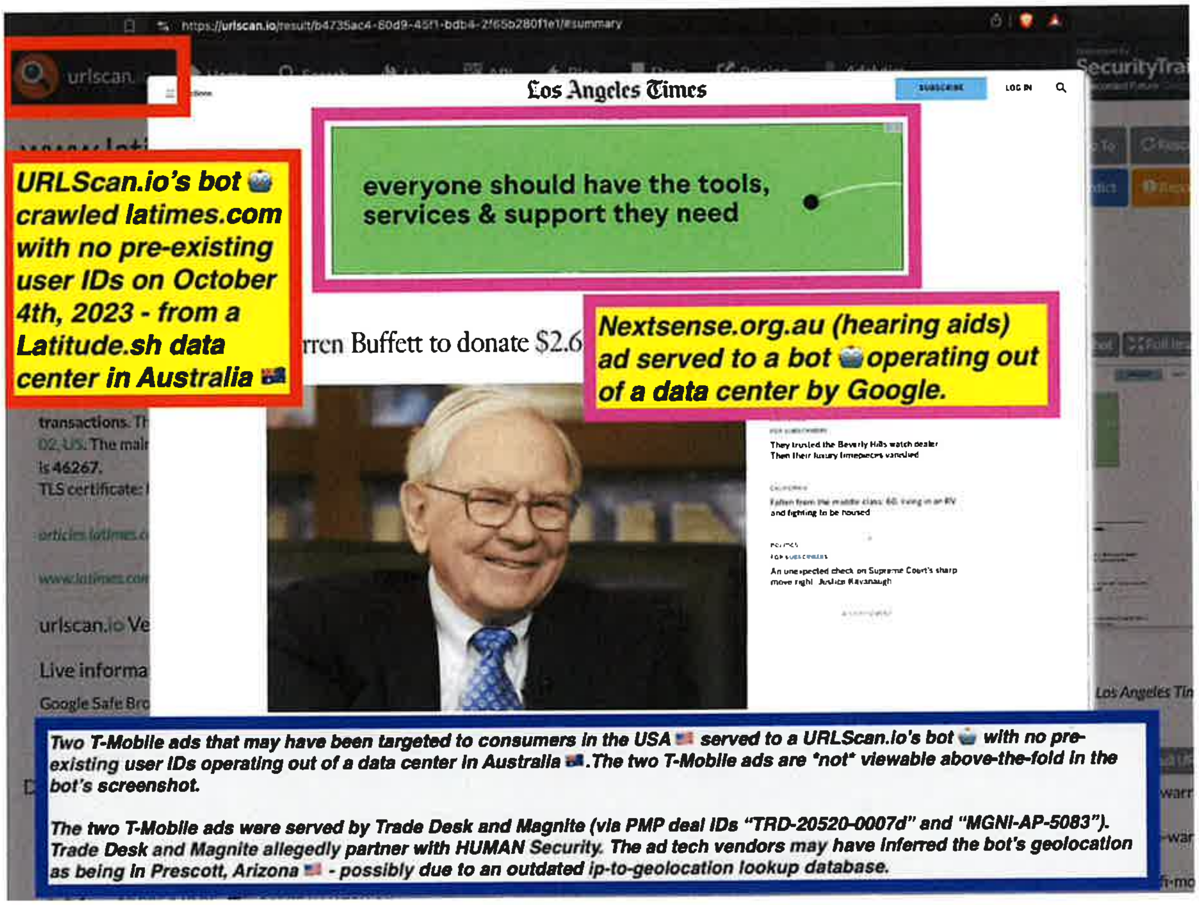
The Diageo ad includes references to DoubleVerify.

[On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?](https://adalytics.io/blog/prebid-bot-filtration)

A Diageo Smirnoff alcohol ad was served to URLScan.io's bot whilst the bot was crawling eliteprospects.com on November 25th, 2024 with no pre-existing user identifiers. The Diageo alcohol ad appears to have been served by Trade Desk and Triplelift (via PMP deal ID "tlx-63903"), both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance". Two HP ads were also served to the bot with no pre-existing user identifiers. Source: https://urlscan.io/result/1a9ca0a9-a7c8-4c45-bb8d-d7f33f39c14a/#summary

As another example, a Nextsense.org.au (hearing aids) ad and two T-Mobile ads were served to URLScan.io's bot whilst the bot was crawling latimes.com on October 4th, 2023 with no pre-existing user identifiers from a data center in Australia. The T-Mobile ads are not viewable above the fold in the screenshot generated by the bot. The T-Mobile ads were served to the bot by Trade Desk and Magnite (via PMP deal ID "TRD-20520-0007d" and "MGNI-AP-5083"), both of whom claim to partner with HUMAN Security.

The T-Mobile ads appear to have been targeted to a consumer in Prescott, Arizona, USA when they were served to a bot in a data center in Australia. This may be due to one or more ad tech vendors using an outdated IP address to geolocation lookup database.


https://urlscan.io/result/b4735ac4-80d9-45f1-bdb4-2f65b280f1e1/#summary
urlscan
Los Angeles Times
SUBSCRIBE
LOG IN
everyone should have the tools, services & support they need
rren Buffett to donate $2.6
They trusted the Beverly Hills watch dealer Then their luxury timepieces vanished
Fallen from the middle class: 60, living in an RV and fighting to be housed
An unexpected check on Supreme Court's sharp move right: Justice Kavanaugh
urlscan.io Ve
Live informa
Google Safe Bro
Los Angeles Tin

URLScan.io's bot 🤖 crawled latimes.com with no pre-existing user IDs on October 4th, 2023 - from a Latitude.sh data center in Australia 🇦🇺

Nextsense.org.au (hearing aids) ad served to a bot 🤖 operating out of a data center by Google.

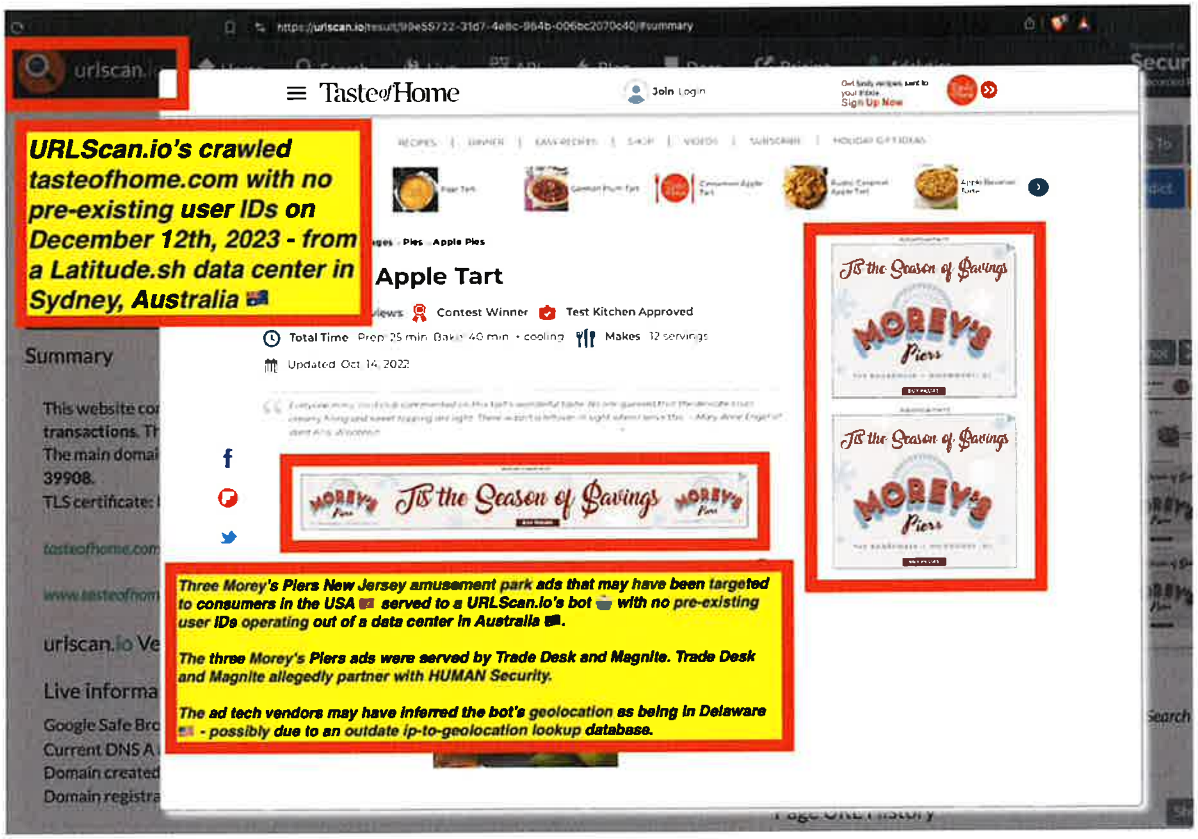
*Two T-Mobile ads that may have been targeted to consumers in the USA 🇺🇸 served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.The two T-Mobile ads are *not* viewable above-the-fold in the bot's screenshot.*

The two T-Mobile ads were served by Trade Desk and Magnite (via PMP deal IDs "TRD-20520-0007d" and "MGNI-AP-5083"). Trade Desk and Magnite allegedly partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Prescott, Arizona 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

A Nextsense.org.au (hearing aids) ad and two T-Mobile ads were served to URLScan.io's bot whilst the bot was crawling latimes.com on October 4th, 2023 with no pre-existing user identifiers from a data center in Australia. The T-Mobile ads are not viewable above the fold in the screenshot generated by the bot. The T-Mobile ads were served to the bot by Trade Desk and Magnite (via PMP deal ID "TRD-20520-0007d" and "MGNI-AP-5083"), both of whom claim to partner with HUMAN Security. The T-Mobile ads appear to have been targeted to a consumer in Prescott, Arizona, USA when they were served to a bot in a data center in Australia. This may be due to one or more ad tech vendors using an outdated IP address to geolocation lookup database. Source: https://urlscan.io/result/b4735ac4-80d9-45f1-bdb4-2f65b280f1e1/#summary

As another example, three Morey's Pier New Jersey amusement park ads were served to URLScan.io's bot whilst the bot was crawling tasteofhome.com on December 12th, 2023 with no pre-existing user identifiers from a data center in Australia. The three Morey's Pier ads were served to the bot by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.

The three Morey's Pier ads appear to have been targeted to a consumer in Delaware, USA when they were served to a bot in a data center in Australia. This may be due to one or more ad tech vendors using an outdated IP address to geolocation lookup database.



URLScan.io's crawled tasteofhome.com with no pre-existing user IDs on December 12th, 2023 - from a Latitude.sh data center in Sydney, Australia 🇦🇺

Three Morey's Piers New Jersey amusement park ads that may have been targeted to consumers in the USA 🇺🇸 served to a URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.

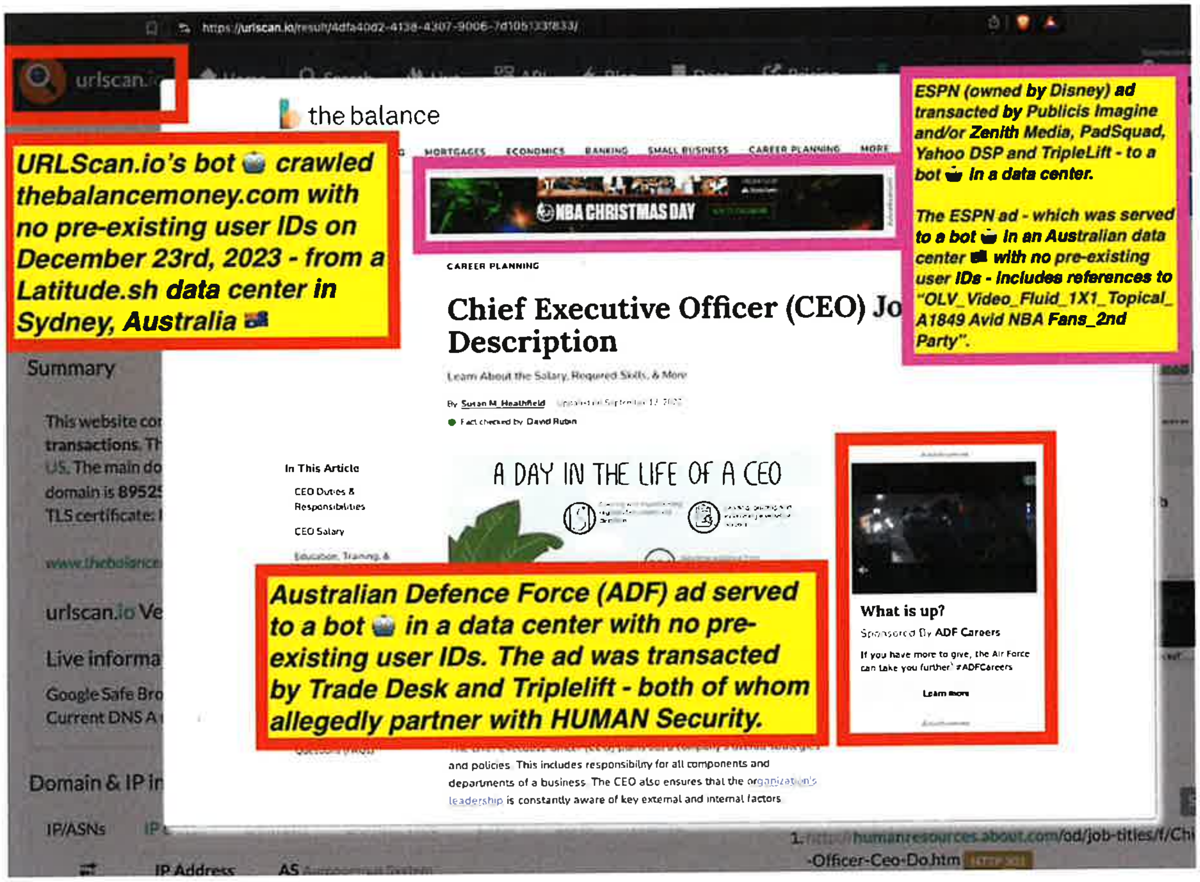
The three Morey's Piers ads were served by Trade Desk and Magnite. Trade Desk and Magnite allegedly partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Delaware 🇺🇸 - possibly due to an outdate ip-to-geolocation lookup database.

Three Morey's Pier New Jersey amusement park ads were served to URLScan.io's bot whilst the bot was crawling tasteofhome.com on December 12th, 2023 with no pre-existing user identifiers from a data center in Australia. The three Morey's Pier ads ads were served to the bot by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security. The three Morey's Pier ads appear to have been targeted to a consumer in Delaware, USA when they were served to a bot in a data center in Australia. This may be due to one or more ad tech vendors using an outdated IP address to geolocation lookup database.

Source: https://urlscan.io/result/99e55722-31d7-4e8c-964b-006bc2070c40/#summary

As another example, an Australian Defence Forces (ADF) government ad and an ESPN ad were served to URLScan.io's bot whilst the bot was crawling thebalanceofmoney.com on December 23rd, 2023 with no pre-existing user identifiers from a data center in Australia. The Australian government ADF ad was served to the bot by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security. The ESPN (owned by Disney) ad appears to have been transacted by Publicis, Padsquad, Yahoo DSP and Triplelift.



URLScan.io's bot 🤖 crawled thebalancemoney.com with no pre-existing user IDs on December 23rd, 2023 - from a Latitude.sh data center in Sydney, Australia 🇦🇺

ESPN (owned by Disney) ad transacted by Publicis Imagine and/or Zenith Media, PadSquad, Yahoo DSP and TripleLift - to a bot 🤖 in a data center.

The ESPN ad - which was served to a bot 🤖 in an Australian data center 🏢 with no pre-existing user IDs - includes references to "OLV_Video_Fluid_1X1_Topical_A1849 Avid NBA Fans_2nd Party".

Chief Executive Officer (CEO) Jo Description

Learn About the Salary, Required Skills, & More

By Susan M. Heathfield

Fact checked by David Rubin

Australian Defence Force (ADF) ad served to a bot 🤖 in a data center with no pre-existing user IDs. The ad was transacted by Trade Desk and Triplelift - both of whom allegedly partner with HUMAN Security.

What is up?

Sponsored By ADF Careers

If you have more to give, the Air Force can take you further' #ADFCareers

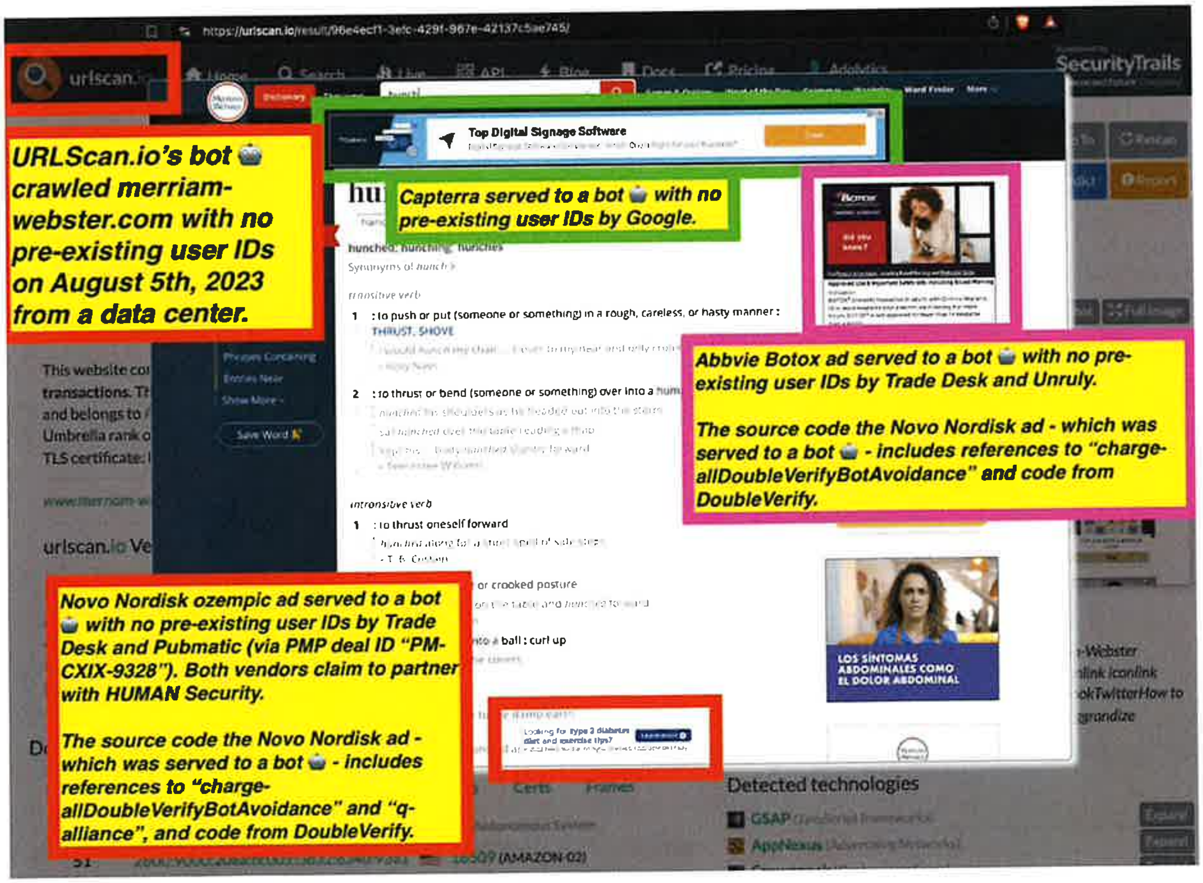
and policies. This includes responsibility for all components and departments of a business. The CEO also ensures that the organization's leadership is constantly aware of key external and internal factors

An Australian Defence Forces (ADF) government ad and an ESPN ad were served to URLScan.io's bot whilst the bot was crawling thebalanceofmoney.com on December 23rd, 2023 with no pre-existing user identifiers from a data center in Australia. The Australian government ADF ad was served to the bot by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security. The ESPN (owned *by Disney) ad appears to have been transacted by Publicis, Padsquad, Yahoo DSP and Triplelift. Source: https://urlscan.io/result/4dfa40d2-4138-4307-9006-7d105133f833/#summary*

As another example, an Novo Nordisk Ozempic ad, an Abbvie Botox ad, and a Capterra ad were served to URLScan.io's bot whilst the bot was crawling merriam-webster.com on August 5th, 2023 with no pre-existing user identifiers.

The Novo Nordisk Ozempic ad was served to a bot by Trade Desk and Pubmatic (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security. The source code of the Novo Nordisk ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

The Abbvie Botox ad was served to a bot by Trade Desk and Unruly. The source code of the Abbvie Botox ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.



https://urlscan.io/result/96e4ecf1-3efc-4291-967e-42137c5ae745/

URLScan.io's bot 🤖 crawled merriam-webster.com with no pre-existing user IDs on August 5th, 2023 from a data center.

Capterra served to a bot 🤖 with no pre-existing user IDs by Google.

Abbvie Botox ad served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Unruly.

The source code the Novo Nordisk ad - which was served to a bot 🤖 - includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

Novo Nordisk ozempic ad served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Pubmatic (via PMP deal ID "PM-CXIX-9328"). Both vendors claim to partner with HUMAN Security.

The source code the Novo Nordisk ad - which was served to a bot 🤖 - includes references to "charge-allDoubleVerifyBotAvoidance" and "q-alliance", and code from DoubleVerify.

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Adalytics
SecurityTrails
Top Digital Signage Software
hunched; hunching; hunches
Synonyms of hunch
transitive verb
1 : to push or put (someone or something) in a rough, careless, or hasty manner :
THRUST, SHOVE
2 : to thrust or bend (someone or something) over into a hump
intransitive verb
1 : to thrust oneself forward
or crooked posture
into a ball : curl up
LOS SÍNTOMAS ABDOMINALES COMO EL DOLOR ABDOMINAL
Looking for type 2 diabetes diet and exercise tips?
Detected technologies
GSAP
AppNexus
urlscan.io Ve
AMAZON-02

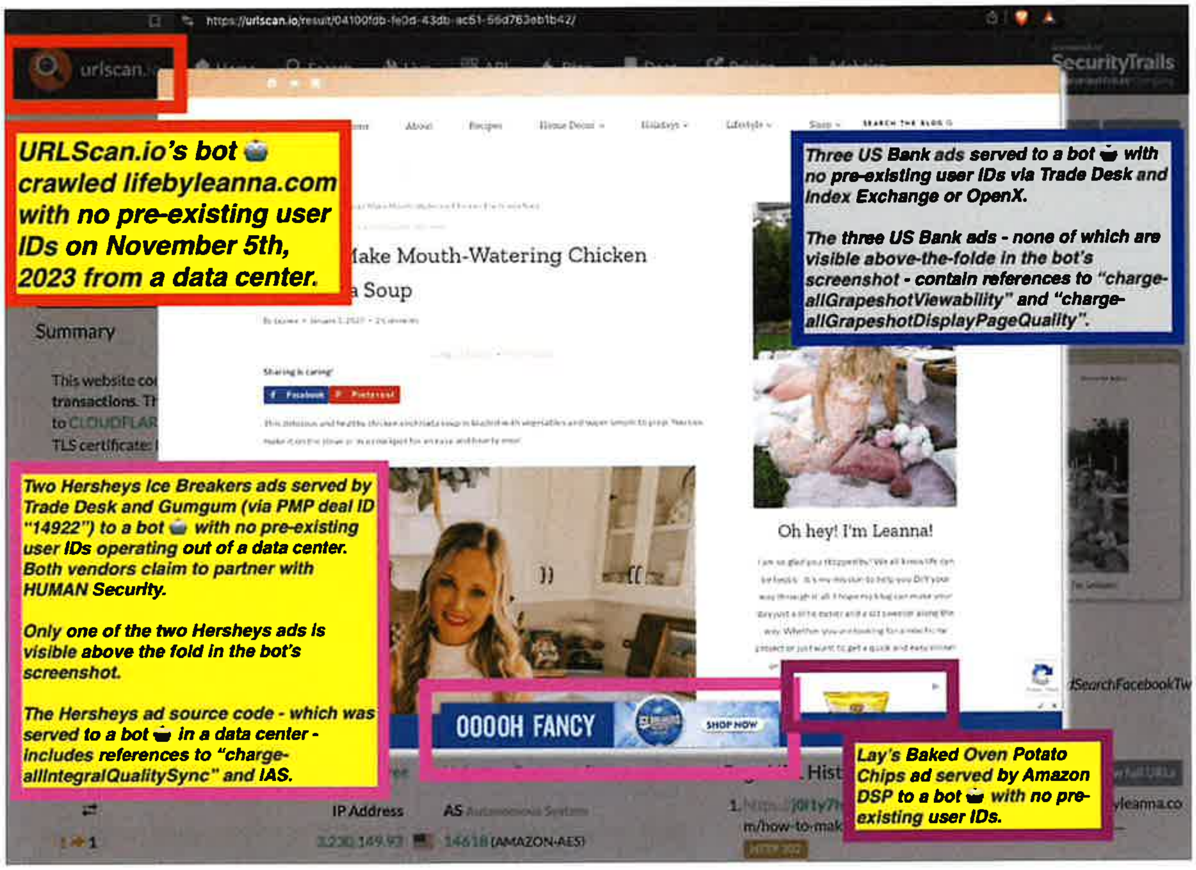
A Novo Nordisk Ozempic ad, an Abbvie Botox ad, and a Capterra ad were served to URLScan.io's bot whilst the bot was crawling merriam-webster.com on August 5th, 2023 with no pre-existing user identifiers. The Novo Nordisk ozempic ad was served to a bot by Trade Desk and Pubmatic (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security. The source code of the Novo Nordisk ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. The Abbvie Botox ad was served to a bot by Trade Desk and Unruly. The source code of the Abbvie Botox ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. Source: https://urlscan.io/result/96e4ecf1-3efc-429f-967e-42137c5ae745/

As another example, two Hershey's Ice Breakers, three US Bank ads and a Lay's Baked Oven Potato Chips ad were served to URLScan.io's bot whilst the bot was crawling lifebyleanna.com on November 5th, 2023 from a data center with no pre-existing user identifiers. Several of the ads are not visible above-the-fold in the screenshot generated by the bot.

The Hershey's ads were served by Trade Desk and GumGum (via PMP deal ID "14922"), both of whom claim to partner with HUMAN Security. The source code of the Hershey's ads that were served to a bot include references to IAS and "charge-allIntegralQualitySync".

The three US Bank ads - none of which are visible above-the-fold in the screenshot generated by the bot - appear to have been transacted by Trade Desk, Index Exchange, and OpenX - all three of whom claim to partner with HUMAN Security. The source code of the three US Bank ads include references to "charge-allGrapeshotVieawbility" and "charge-allGrapeshotDisplayPageQuality".

The Lay's Baked Oven Potato Chips ad appears to have been transacted by Amazon DSP.



URLScan.io's bot 🤖 crawled lifebyleanna.com with no pre-existing user IDs on November 5th, 2023 from a data center.

Three US Bank ads served to a bot 🤖 with no pre-existing user IDs via Trade Desk and Index Exchange or OpenX.

The three US Bank ads - none of which are visible above-the-folde in the bot's screenshot - contain references to "charge-allGrapeshotViewability" and "charge-allGrapeshotDisplayPageQuality".

Two Hersheys Ice Breakers ads served by Trade Desk and Gumgum (via PMP deal ID "14922") to a bot 🤖 with no pre-existing user IDs operating out of a data center. Both vendors claim to partner with HUMAN Security.

Only one of the two Hersheys ads is visible above the fold in the bot's screenshot.

The Hersheys ad source code - which was served to a bot 🤖 in a data center - includes references to "charge-allIntegralQualitySync" and IAS.

Lay's Baked Oven Potato Chips ad served by Amazon DSP to a bot 🤖 with no pre-existing user IDs.

https://urlscan.io/result/04100fdb-fe0d-43db-ac51-56d763eb1b42/
urlscan.io
SecurityTrails
Make Mouth-Watering Chicken Soup
Summary
This website co transactions. Th to CLOUDFLAR TLS certificate:
Oh hey! I'm Leanna!
OOOOH FANCY
SHOP NOW
IP Address
AS
14618 (AMAZON-AES)

Two Hershey's Ice Breakers, three US Bank ads and a Lay's Baked Oven Potato Chips ad were served to URLScan.io's bot whilst the bot was crawling lifebyleanna.com on November 5th, 2023 from a data center with no pre-existing user identifiers. Several of the ads are not visible above-the-fold in the screenshot generated by the bot. The Hershey's ads were served by Trade Desk and GumGum (via PMP deal ID "14922"), both of whom claim to partner with HUMAN Security. The source code of the Hershey's ads that were served to a bot include references to IAS and "charge-allIntegralQualitySync". The three US Bank ads - none of which are visible above-the-fold in the screenshot generated by the bot - appear to have been transacted by Trade Desk, Index Exchange, and OpenX - all three of whom claim to partner with HUMAN Security. The source code of the three US Bank ads include references to "charge-allGrapeshotVieawbility" and "charge-allGrapeshotDisplayPageQuality". The Lay's Baked Oven Potato Chips ad appears to have been transacted by Amazon DSP.

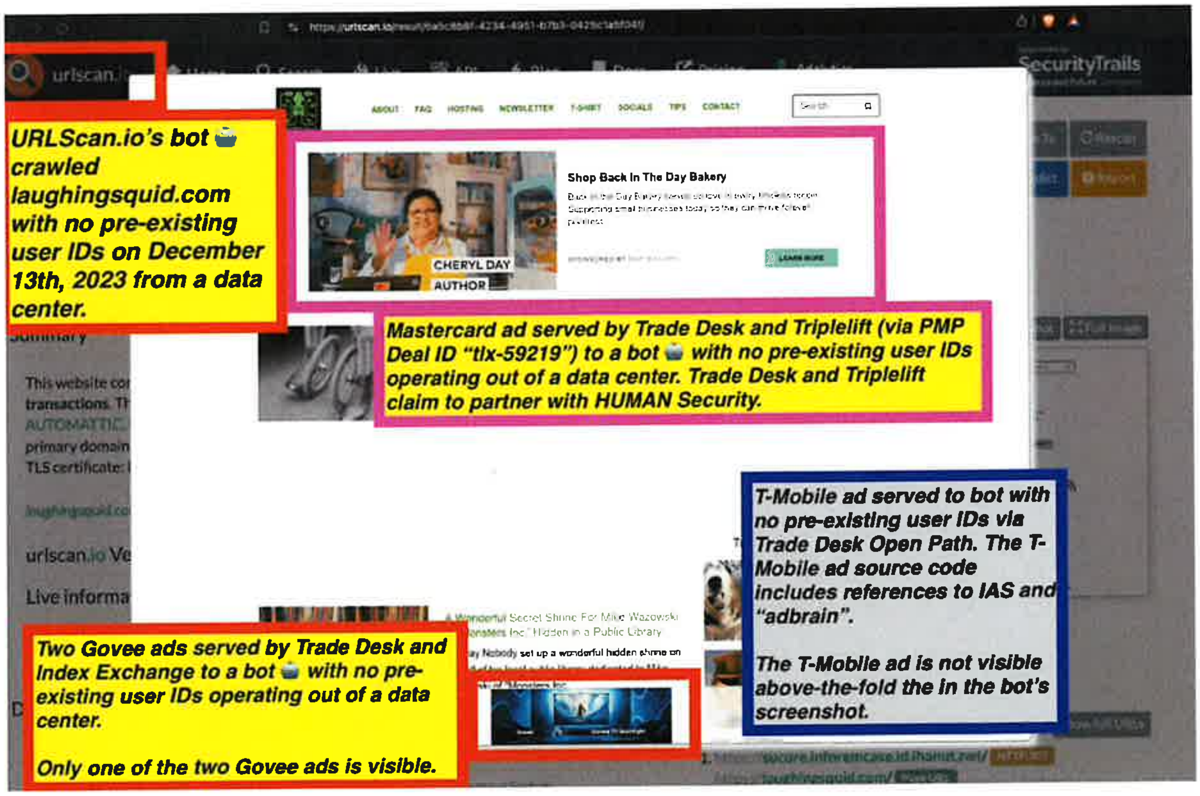
Source: https://urlscan.io/result/04100fdb-fe0d-43db-ac51-56d763eb1b42/#summary

As another example, a Mastercard ad, two Govee ads, and a T-Mobile ad were served to URLScan.io's bot whilst the bot was crawling laughingsquid.com on December 13th, 2023 from a data center with no pre-existing user identifiers.

The Mastercard ad appears to have been transacted by Trade Desk and Triplelift (via PMP deal "tlx-59219"), both of whom claim to partner with HUMAN Security.

The two Govee ads appear to have been served by Trade Desk and Index Exchange. Only one of the two Govee ads is visible above-the-fold in the screenshot generated by the URLScan.io bot.

The T-Mobile ad appears to have been served to the bot by Trade Desk Open Path. The source code of the T-Mobile ad includes references to IAS and "adbrain". The T-Mobile ad is not visible above-the-fold in the screenshot generated by URLScan.io's bot.



urlscan.io
SecurityTrails
ABOUT FAQ HOSTING NEWSLETTER T-SHIRT SOCIALS TIPS CONTACT
Shop Back In The Day Bakery
CHERYL DAY AUTHOR
LEARN MORE
Summary
urlscan.io
Live informa

URLScan.io's bot 🤖 crawled laughingsquid.com with no pre-existing user IDs on December 13th, 2023 from a data center.

Mastercard ad served by Trade Desk and Triplelift (via PMP Deal ID "tlx-59219") to a bot 🤖 with no pre-existing user IDs operating out of a data center. Trade Desk and Triplelift claim to partner with HUMAN Security.

T-Mobile ad served to bot with no pre-existing user IDs via Trade Desk Open Path. The T-Mobile ad source code includes references to IAS and "adbrain".

The T-Mobile ad is not visible above-the-fold the in the bot's screenshot.

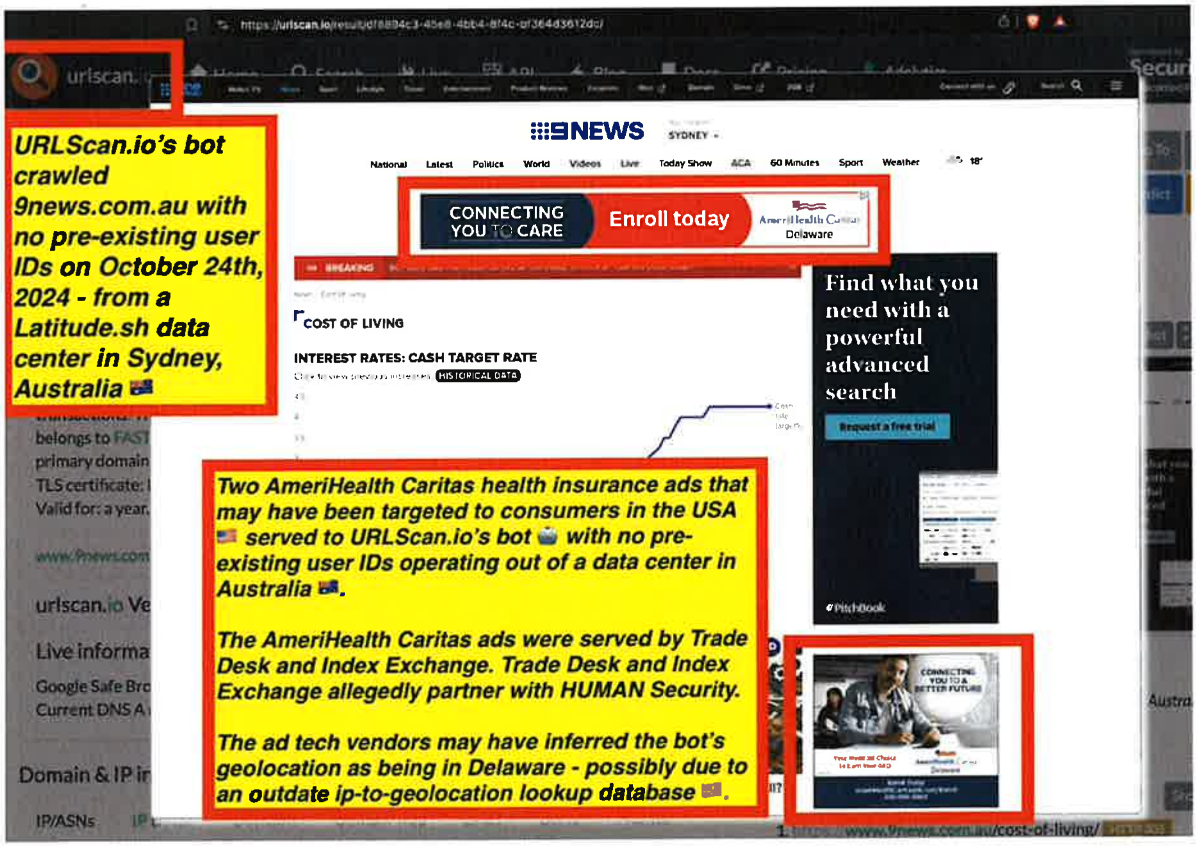
Two Govee ads served by Trade Desk and Index Exchange to a bot 🤖 with no pre-existing user IDs operating out of a data center.

Only one of the two Govee ads is visible.

A Mastercard ad, two Govee ads, and a T-Mobile ad were served to URLScan.io's bot whilst the bot was crawling laughinsquid.com on December 13th, 2023 from a data center with no pre-existing user identifiers. Source: https://urlscan.io/result/6a5c8b8f-4234-4951-b7b3-0425c1a5f04f/

As another example, two AmeriHealth Caritas health insurance ads were served to URLScan.io's bot whilst the bot was crawling 9news.com.au on October 24th, 2024 from a data center in Australia with no pre-existing user identifiers. The AmeriHealth Caritas ads appear to have been transacted by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security.

The AmeriHealth Caritas health insurance ads appear to have been targeted to a consumer in Delaware, USA when they were served to a bot in a data center in Australia. It is possible that one or more ad tech vendors are using an out-dated IP address-to-geolocation lookup database.



URLScan.io's bot crawled 9news.com.au with no pre-existing user IDs on October 24th, 2024 - from a Latitude.sh data center in Sydney, Australia 🇦🇺

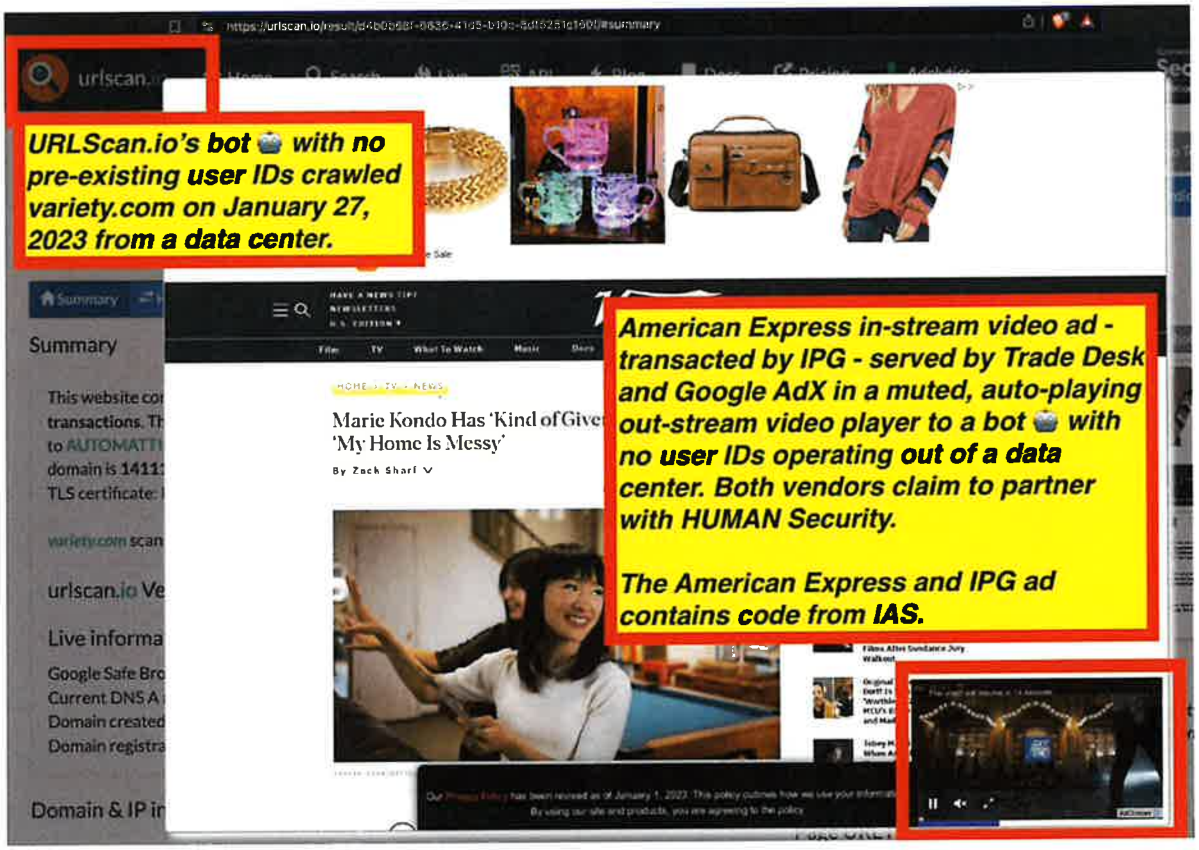
Two AmeriHealth Caritas health insurance ads that may have been targeted to consumers in the USA 🇺🇸 served to URLScan.io's bot 🤖 with no pre-existing user IDs operating out of a data center in Australia 🇦🇺.

The AmeriHealth Caritas ads were served by Trade Desk and Index Exchange. Trade Desk and Index Exchange allegedly partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Delaware - possibly due to an outdate ip-to-geolocation lookup database 🇺🇸.

Two AmeriHealth Caritas health insurance ads were served to URLScan.io's bot whilst the bot was crawling 9news.com.au on October 24th, 2024 from a data center in Australia with no pre-existing user identifiers. The AmeriHealth Caritas ads appear to have been transacted by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security. Source: https://urlscan.io/result/df8894c3-45e8-4bb4-8f4c-bf364d3612dc/

As another example, an American Express video ad was served to URLScan.io's bot whilst the bot was crawling variety.com on January 27th, 2023 from a data center with no pre-existing user identifiers. The American Express ad appears to have been transacted by IPG media agency, Trade Desk and Google AdX. The American Express ad contains code from IAS.



URLScan.io's bot* 🤖 *with no pre-existing user IDs crawled variety.com on January 27, 2023 from a data center.

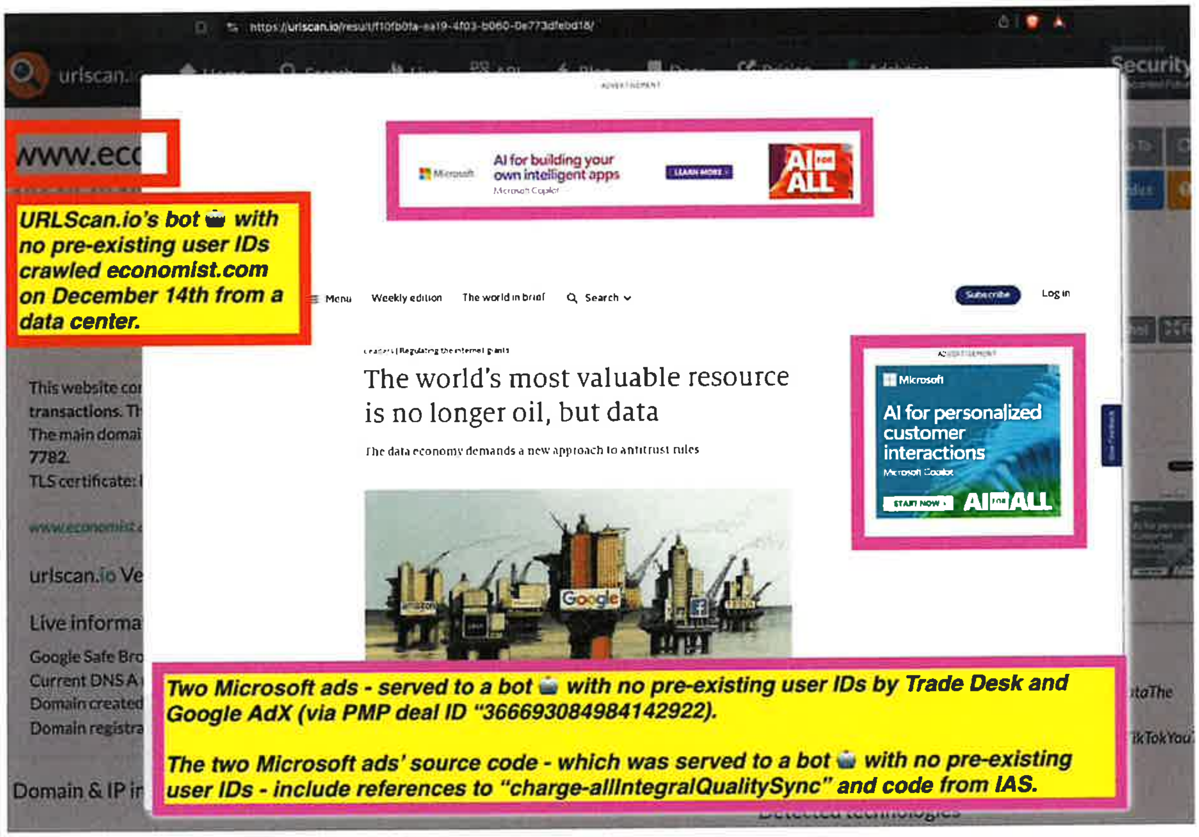
American Express in-stream video ad - transacted by IPG - served by Trade Desk and Google AdX in a muted, auto-playing out-stream video player to a bot* 🤖 *with no user IDs operating out of a data center. Both vendors claim to partner with HUMAN Security.

The American Express and IPG ad contains code from IAS.

An American Express video ad was served to URLScan.io's bot whilst the bot was crawling variety.com on January 27th, 2023 from a data center with no pre-existing user identifiers. The American Express ad appears to have been transacted by IPG media agency, Trade Desk and Google

AdX. The American Express ad contains code from IAS. Source: https://urlscan.io/result/d4b0b68f-6636-41d5-b10c-8df5251c160f/

As another example, two Microsoft ads were served to URLScan.io's bot whilst the bot was crawling economist.com on December 14th, 2017 from a Nexeon data center with no pre-existing user IDs. The Microsoft ads appear to have been served by Trade Desk and Google AdX (via PMP deal ID "3666930849841429 22"). The source code of the Microsoft ads that were served to a bot in a data center contain references to IAS and to "charge-allIntegralQualitySync".



URLScan.io's bot 🤖 with no pre-existing user IDs crawled economist.com on December 14th from a data center.

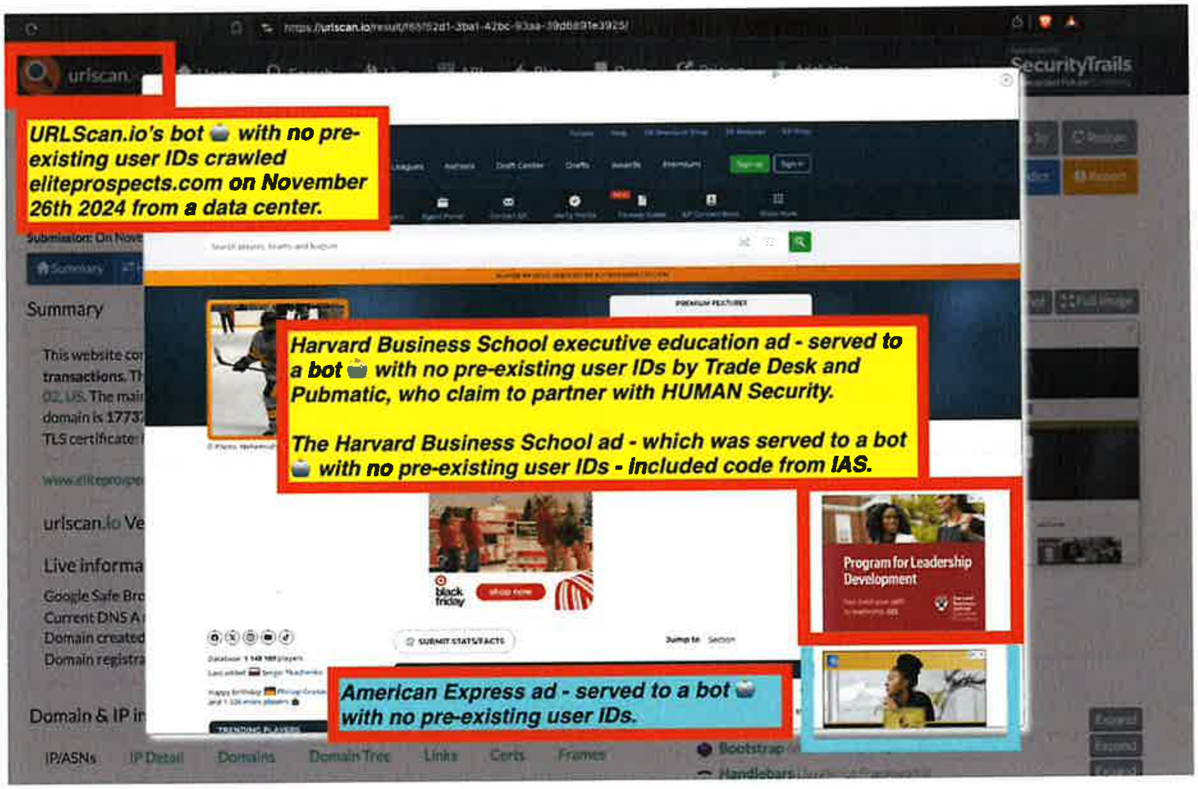
Two Microsoft ads - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Google AdX (via PMP deal ID "3666930849841429 22).

The two Microsoft ads' source code - which was served to a bot 🤖 with no pre-existing user IDs - include references to "charge-allIntegralQualitySync" and code from IAS.

Two Microsoft ads were served to URLScan.io's bot whilst the bot was crawling economist.com on December 14th, 2017 from a Nexeon data center with no pre-existing user IDs. The Microsoft ads appear to have been served by Trade Desk and Google AdX (via PMP deal ID "3666930849841429 22"). The source code of the Microsoft ads that were served to a bot in a data center contain references to IAS and to "charge-allIntegralQualitySync". Source:

https://urlscan.io/result/f10fb0fa-ea19-4f03-b060-0e773dfebd18/#summary

As another example, a Harvard Business School executive education ad and an American Express ad were served to URLScan.io's bot whilst it was crawling eliteprospects.com on November 26th, 2024. The Harvard Business School ad appears to have been transacted by Trade Desk and Pubmatic, both of whom partner with HUMAN Security. The Harvard Business School ad that was served to a bot includes code from IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled eliteprospects.com on November 26th 2024 from a data center.

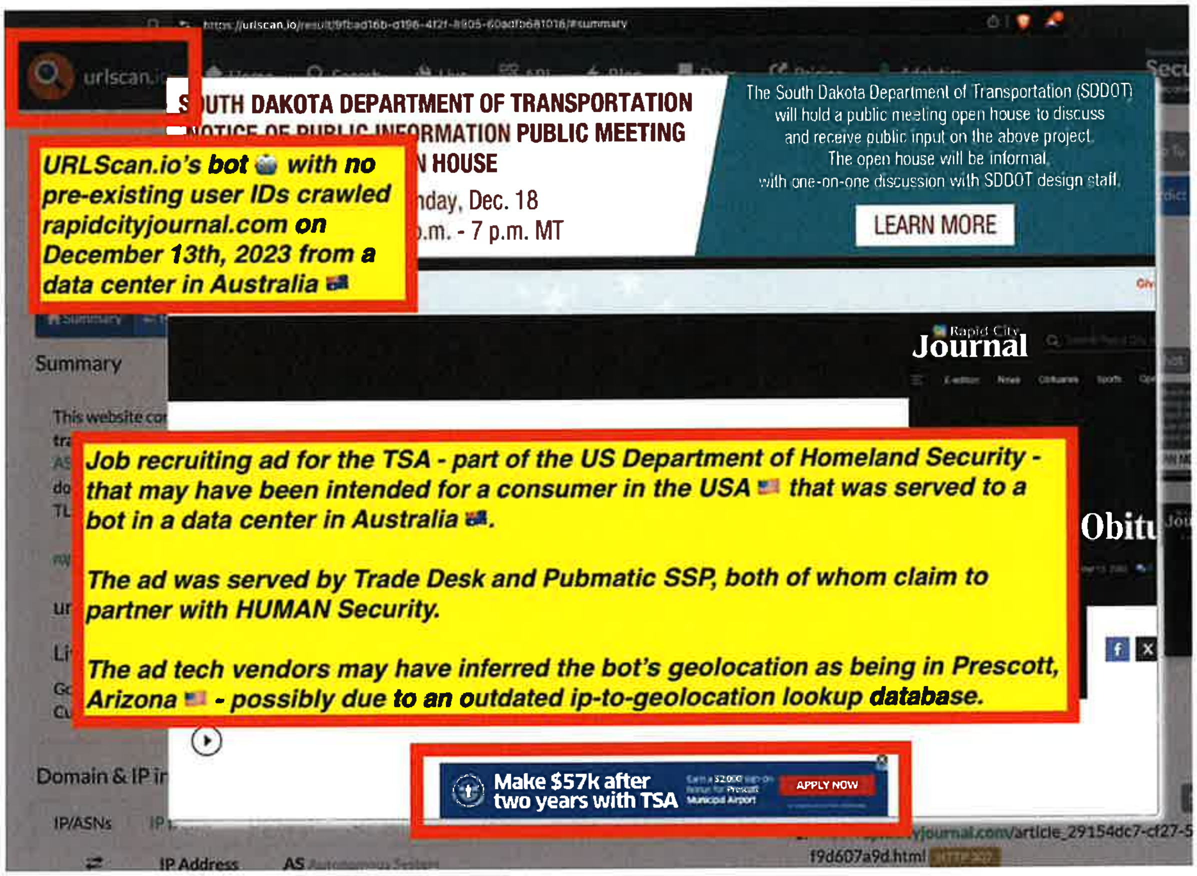
Harvard Business School executive education ad - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Pubmatic, who claim to partner with HUMAN Security.

The Harvard Business School ad - which was served to a bot 🤖 with no pre-existing user IDs - included code from IAS.

American Express ad - served to a bot 🤖 with no pre-existing user IDs.

A Harvard Business School executive education ad and an American Express ad were served to URLScan.io's bot whilst it was crawling eliteprospects.com on November 26th, 2024. The Harvard Business School ad appears to have been transacted by Trade Desk and Pubmatic, both of whom partner with HUMAN Security. The Harvard Business School ad that was served to a bot includes code from IAS. Source: https://urlscan.io/result/f65f52d1-3ba1-42bc-93aa-39d6891e3925/#summary

As another example, a Transportation Security Administration (TSA) Department of Homeland Security (DHS) ad that was served to URLScan.io's bot whilst it was crawling rapidcityjournal.com on December 13th, 2023. The TSA ad appears to have been transacted by Trade Desk and Pubmatic, both of whom partner with HUMAN Security.



URLScan.io's **bot** with **no** pre-existing user IDs crawled rapidcityjournal.com **on** December 13th, 2023 from **a** data center in Australia

Job recruiting ad for the TSA - part of the US Department of Homeland Security - that may have been intended for a consumer in the USA that was served to a bot in a data center in Australia.

The ad was served by Trade Desk and Pubmatic SSP, both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Prescott, Arizona - possibly due **to an** outdated ip-to-geolocation lookup **database.**

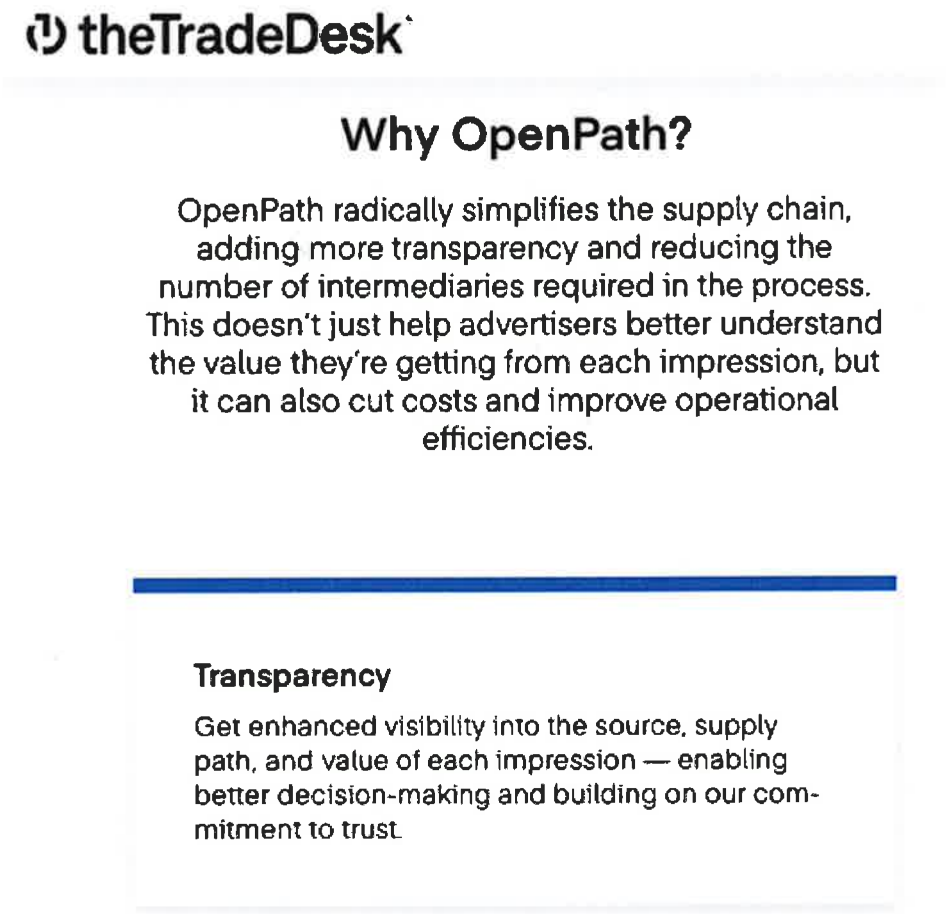
urlscan.io
SOUTH DAKOTA DEPARTMENT OF TRANSPORTATION
NOTICE OF PUBLIC INFORMATION PUBLIC MEETING
N HOUSE
nday, Dec. 18
.m. - 7 p.m. MT
The South Dakota Department of Transportation (SDDOT) will hold a public meeting open house to discuss and receive public input on the above project. The open house will be informal, with one-on-one discussion with SDDOT design staff.
LEARN MORE
Summary
Rapid City Journal
Obitu
Domain & IP ir
IP/ASNs
IP Address
AS
Make $57k after two years with TSA
Earn a $2,000 sign-on bonus for Prescott Municipal Airport
APPLY NOW
journal.com/article_29154dc7-cf27-5
f9d607a9d.html

Screenshot of a Transportation Security Administration (TSA) job recruiting ad, served to a bot in Australia. TSA is part of the US Department of Homeland Security. Source: https://urlscan.io/result/9fbad16b-d196-4f2f-8905-60adfb681016/#summary

Ads served by Trade Desk Open Path to declared bots on the IAB Bots List operating out of known data center IP addresses

Over 1700 different brands and advertisers were observed as transacting via Trade Desk Open Path and having their ads served to declared bots (whose user agent is on the IAB Tech Lab Spiders and

Bots list since 2013) operating out of well known data center IP addresses. Open Path is a Trade Desk initiative that circumvents traditional supply side platforms, and gives media buyers direct access to inventory sold by publishers to the Trade Desk DSP.



theTradeDesk

Why OpenPath?

OpenPath radically simplifies the supply chain, adding more transparency and reducing the number of intermediaries required in the process. This doesn't just help advertisers better understand the value they're getting from each impression, but it can also cut costs and improve operational efficiencies.

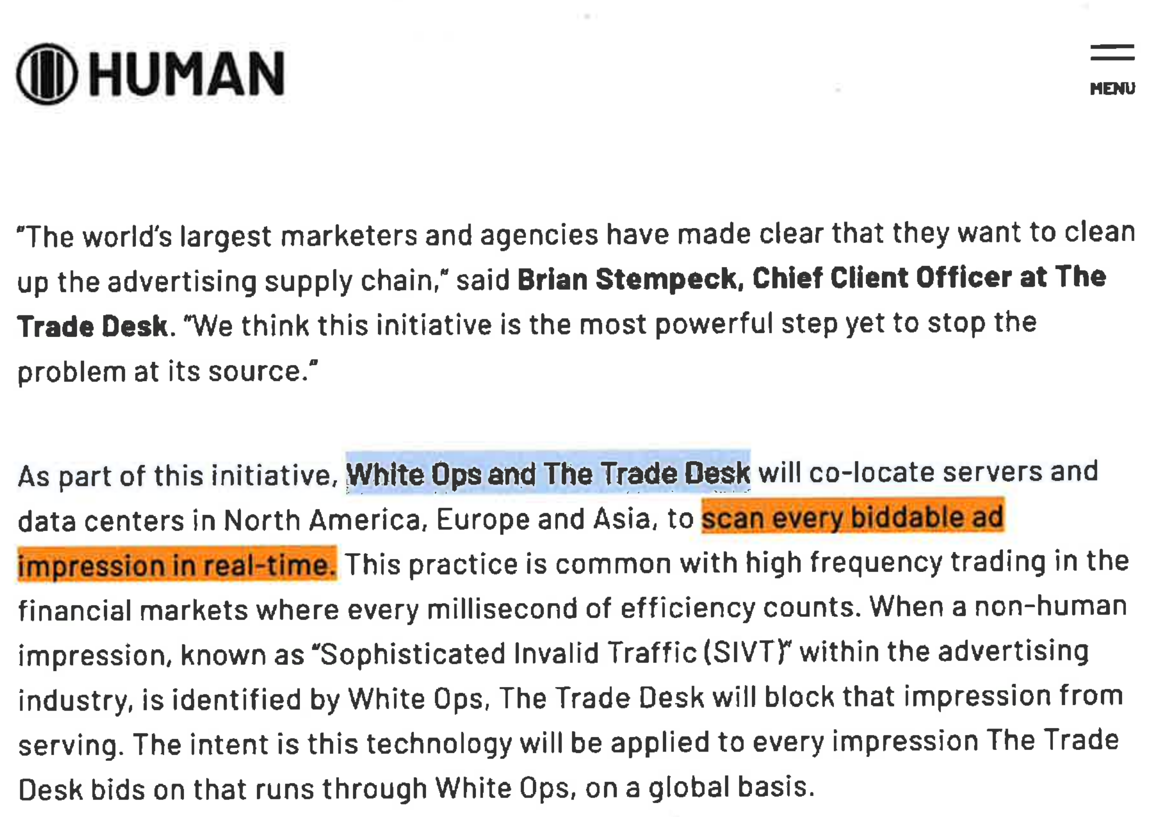
Transparency

Get enhanced visibility into the source, supply path, and value of each impression — enabling better decision-making and building on our commitment to trust.

Screenshot of the Trade Desk Open Path page - https://www.thetradedesk.com/us/our-platform/openpath

It is not immediately apparent from Trade Desk's public documentation whether Trade Desk Open Path scans every ad impression pre-bid with HUMAN Security's MediaGuard before deciding to serve a clients' ad to a declared bot in a data center.

However, Trade Desk previously announced that it would "scan every biddable ad impression in real-time" using HUMAN Security's tools.



"The world's largest marketers and agencies have made clear that they want to clean up the advertising supply chain," said **Brian Stempeck, Chief Client Officer at The Trade Desk**. "We think this initiative is the most powerful step yet to stop the problem at its source."

As part of this initiative, White Ops and The Trade Desk will co-locate servers and data centers in North America, Europe and Asia, to scan every biddable ad impression in real-time. This practice is common with high frequency trading in the financial markets where every millisecond of efficiency counts. When a non-human impression, known as "Sophisticated Invalid Traffic (SIVT)" within the advertising industry, is identified by White Ops, The Trade Desk will block that impression from serving. The intent is this technology will be applied to every impression The Trade Desk bids on that runs through White Ops, on a global basis.

Screenshot of a joint Trade Desk and HUMAN Security (f/k/a White Ops) press release

The list of advertisers whose ads were served by Trade Desk Open Path to declared bots (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP addresses included Progressive insurance, P&G, T-Mobile, Hershey's, Royal Caribbean, Walmart, US Bank, Wawa, Kimberly-Clark, the Government of DC, Unilever, American Airlines, UPS, Coca-Cola, Subaru, Sling, Samsung, H&R Block, Microsoft, Chewy, Prudential, Abbvie, Sherwin-Williams, Best Buy, Enterprise car rental, Amazon, Google Fiber, Hilton hotels, Nestle, Lockheed Martin, Starbucks, Western Union, US Cellular, Disney, Thomson Reuters, McDonald's, Cigna, Bayer, American Express, JPMorgan Chase, Henkel, L3Harris, and many others.

For example, T-Mobile had its ads served by Trade Desk Open Path to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP addresses, whilst the bot was crawling the website sweetlittlebluebird.com. The T-

Mobile ad was transacting via PMP Deal ID opath-192-4001-48ha53ha64. In another example, T-Mobile ads were served by Trade Desk Open Path to a declared bot whilst the bot was crawling chelsweets.com. The ad transacted via Deal ID opath-202-4001-r0ygm500ex. At least six different deal IDs were observed transacting T-Mobile ads via Trade Desk Open Path to declared bots on the IAB Bots List operating out of known data center IP addresses. These PMP deal IDs included: opath-192-4001-48ha53ha64', 'opath-192-4001-3j23aoyt60', "opath-202-4001-bw61qpmbmy', 'opath-202-4001-82coeyei2u', 'opath-202-4001-r0ygm500ex', and 'opath-220-4001-rfv8cl6e5t'.

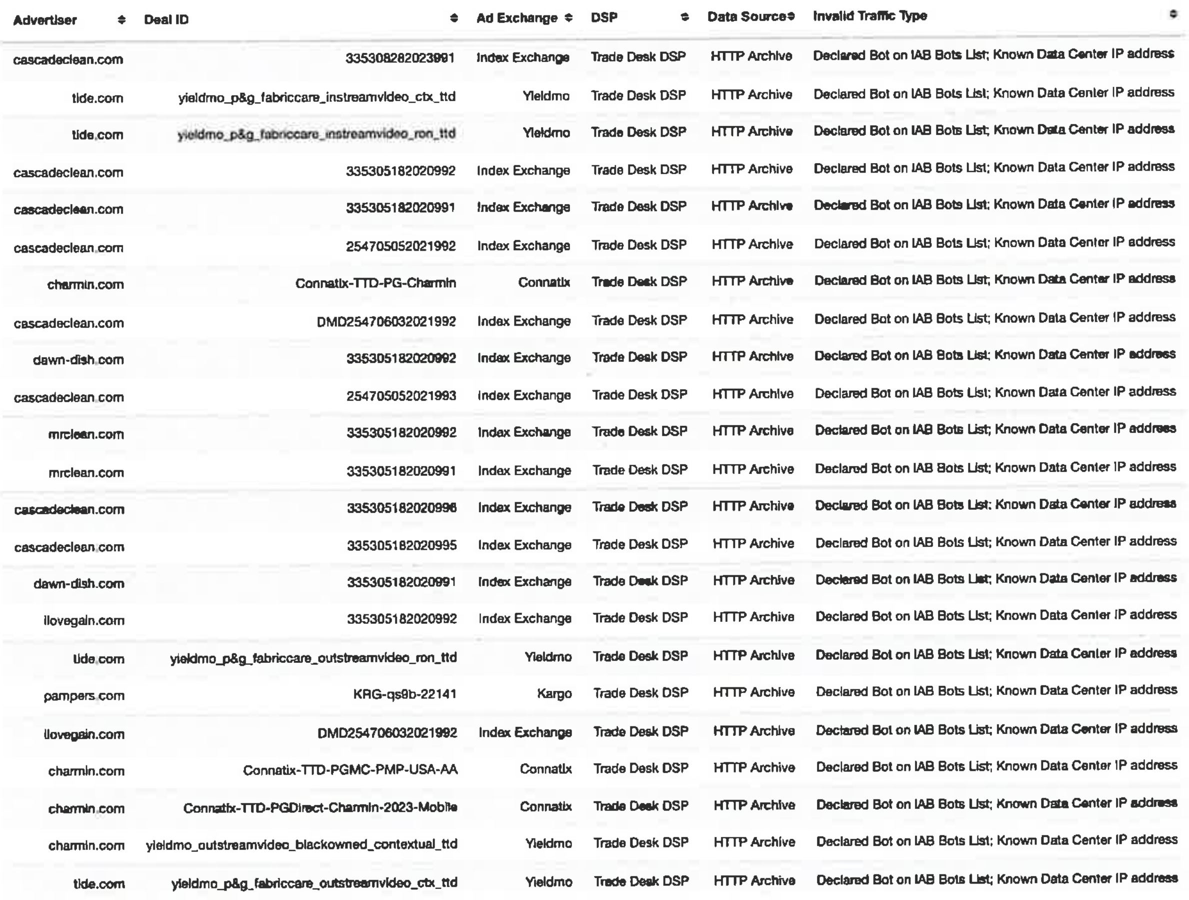
As a second example, Hershey's had its ads served by Trade Desk Open Path to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP addresses, whilst the bot was crawling the website everydaymadefresh.com in December 2022. In another example, Hershey's ads were served by Trade Desk Open Path to a declared bot whilst the bot was crawling asvabpracticetests.com in March, 2024. The ad was transacted via PMP deal ID "3409-192-all-1".

As a third example, Procter & Gamble (P&G) had its ads served by Trade Desk Open Path to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP addresses, whilst the bot was crawling the website reciperunner.com in November 2022. The P&G ad was for the Mr Clean product line. In another example, P&G ads were served by Trade Desk Open Path to a declared bot whilst the bot was crawling littlelearningcorner.com in October, 2023. The P&G ad was for the Pampers product line.

Private marketplace (PMP) and other curated ad deals served to bots by vendors which allegedly partner with HUMAN Security

It appears that many brands who were transacting ad inventory via private marketplace (PMP) or other types of curated ad deals had their ads served to bots.

For example, Procter & Gamble (P&G) had PMPs transacting through Yieldmo and Trade Desk served to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP addresses, via PMP deal IDs “yieldmo_p&g_fabriccare_instreamvideo_ctx_ttd” and “yieldmo_p&g_fabriccare_outstreamvideo_ron_ttd”. The P&G ads were for the Tide product line, and were served to bots crawling websites such as thetravellingtom.com, foodnouveau.com, and vintagerevivals.com. Procter & Gamble (P&G) had ads for Charmin served to declared bots operating out of data centers by Connatix and Trade Desk. The P&G Charmin ads were transacted via PMP deal IDs named “Connatix-TTD-PGDirect-Charmin-2023-Mobile”, “Connatix-TTD-PGMC-PMP-USA-AA”, and “Connatix-TTD-PG-Charmin”.



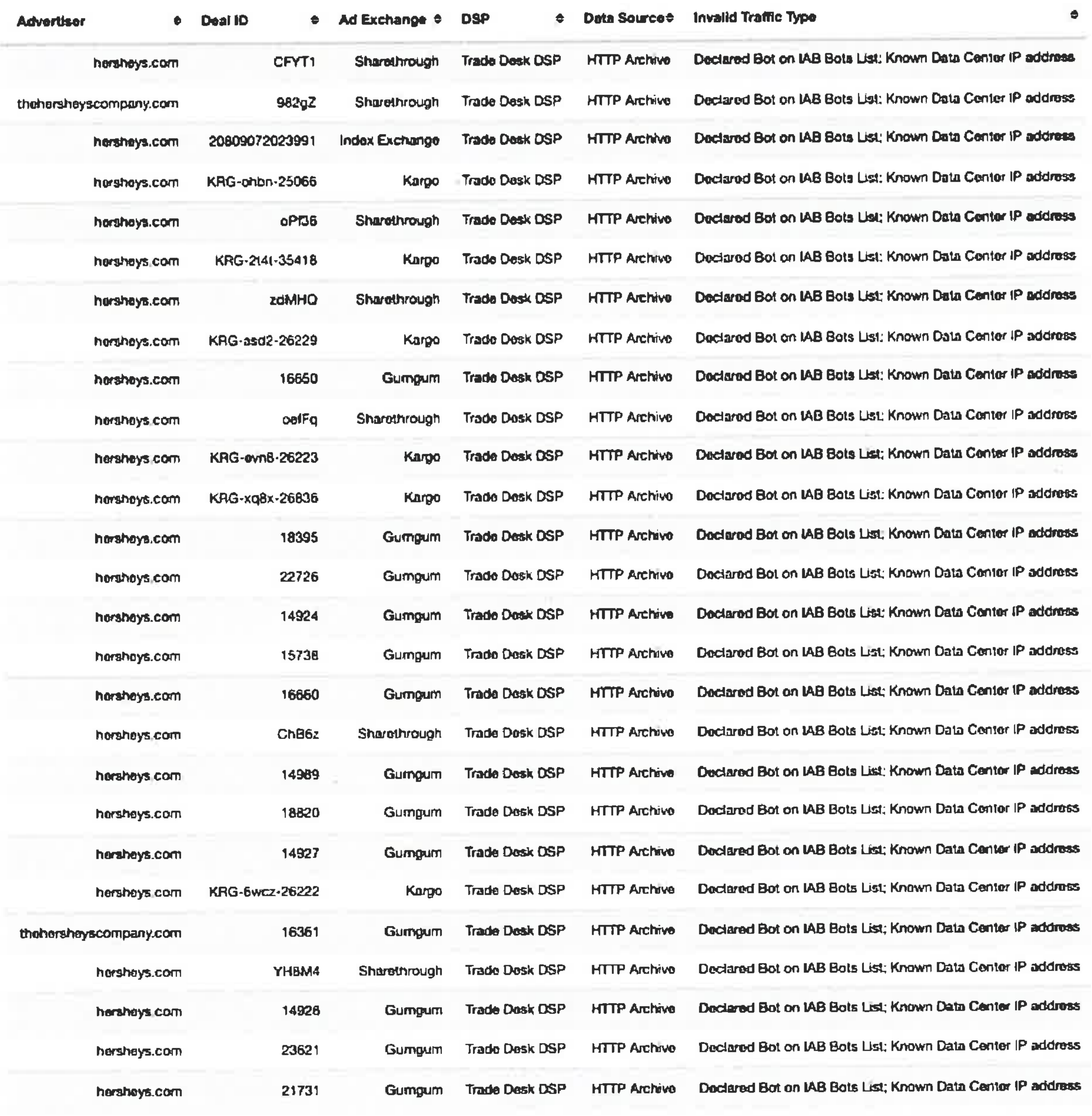
Advertiser ⇕	Deal ID ⇕	Ad Exchange ⇕	DSP ⇕	Data Source⇕	Invalid Traffic Type ⇕
cascadeclean.com	335308282023991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_instreamvideo_ctx_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_instreamvideo_ron_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	254705052021992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
charmin.com	Connatix-TTD-PG-Charmin	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	DMD254706032021992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
dawn-dish.com	335305182020992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	254705052021993	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
mrclean.com	335305182020992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
mrclean.com	335305182020991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020996	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020995	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
dawn-dish.com	335305182020991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
ilovegain.com	335305182020992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_outstreamvideo_ron_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
pampers.com	KRG-qs9b-22141	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
ilovegain.com	DMD254706032021992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
charmin.com	Connatix-TTD-PGMC-PMP-USA-AA	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
charmin.com	Connatix-TTD-PGDirect-Charmin-2023-Mobile	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
charmin.com	yieldmo_outstreamvideo_blackowned_contextual_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_outstreamvideo_ctx_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address

Table illustrating via which PMP deals Procter & Gamble ads were served to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP

As a second example, PepsiCo had ads for Gatorade sports drink served to declared bots operating out of data centers by Yieldmo and Trade Desk. The Gatorade ads were transacted via PMP deal ID named "yieldmo_politicalbuyers_standarddisplay_sportspubs_ttd", and were served to bots crawling websites such as thebusbybabe.sbnation.com and fifaindex.com.

As a third example, alcohol brand Diageo ads served to declared bots operating out of data centers by Yieldmo and Trade Desk. The Diageo ads were transacted via PMP deal IDs named "yieldmo_phdmedia_diageo_donJulio_oustreamvideo_contextual_ttd" and "yieldmo_phd_captainmorgan_instreamvideo_ctx_ttd", and were served to bots crawling websites such as southernliving.com and vegas.eater.com.

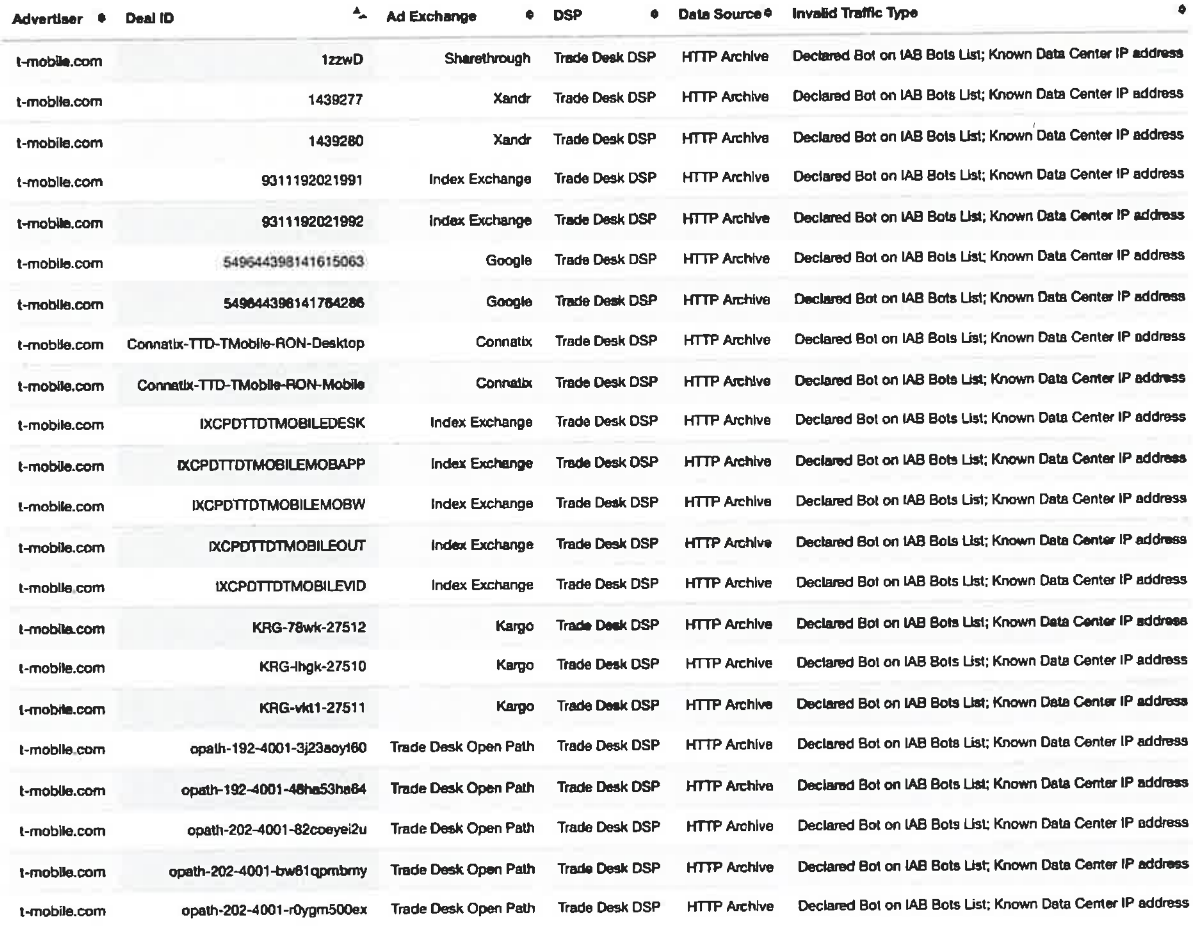
As a fourth example, Hershey's had ads served to declared bots operating out of data center IPs by GumGum, Index Exchange, Kargo, ShareThrough, Microsoft Xandr, and Trade Desk. The Hershey's ads served to bots via GumGum were transacted via PMP deal IDs 16650, 22726, 18820, 16660, and others; Hershey's ads were served to bots via Index Exchange via PMP deal IDs 20809072023991 and 320809082023991; Hershey's ads were served to bots via Kargo PMP deal IDs KRG-ohbn-25066, KRG-2t4t-35418, KRG-asd2-26229, KRG-xq8x-26836, KRG-6wcz-26222, and others; Hershey's ads were served to bots via ShareThrough PMP deal IDs CFYT1, 982gZ, oPf36, zdMHQ, oefFq, erCDb, YH8M4, and others; Hershey's PMP deal IDs were served to bots via Microsoft Xandr PMP deal IDs 1297203 and 1512079.



Advertiser	Deal ID	Ad Exchange	DSP	Data Source	Invalid Traffic Type
hersheys.com	CFYT1	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
thehersheyscompany.com	982gZ	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	20809072023991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-ohbn-25066	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	oPf36	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-2t4t-35418	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	zdMHQ	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-asd2-26229	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	16650	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	oelFq	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-evn8-26223	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-xq8x-26836	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	18395	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	22726	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	14924	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	15738	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	16660	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	ChB6z	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	14989	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	18820	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	14927	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	KRG-6wcz-26222	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
thehersheyscompany.com	16361	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	YHBM4	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	14926	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	23621	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	21731	Gumgum	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address

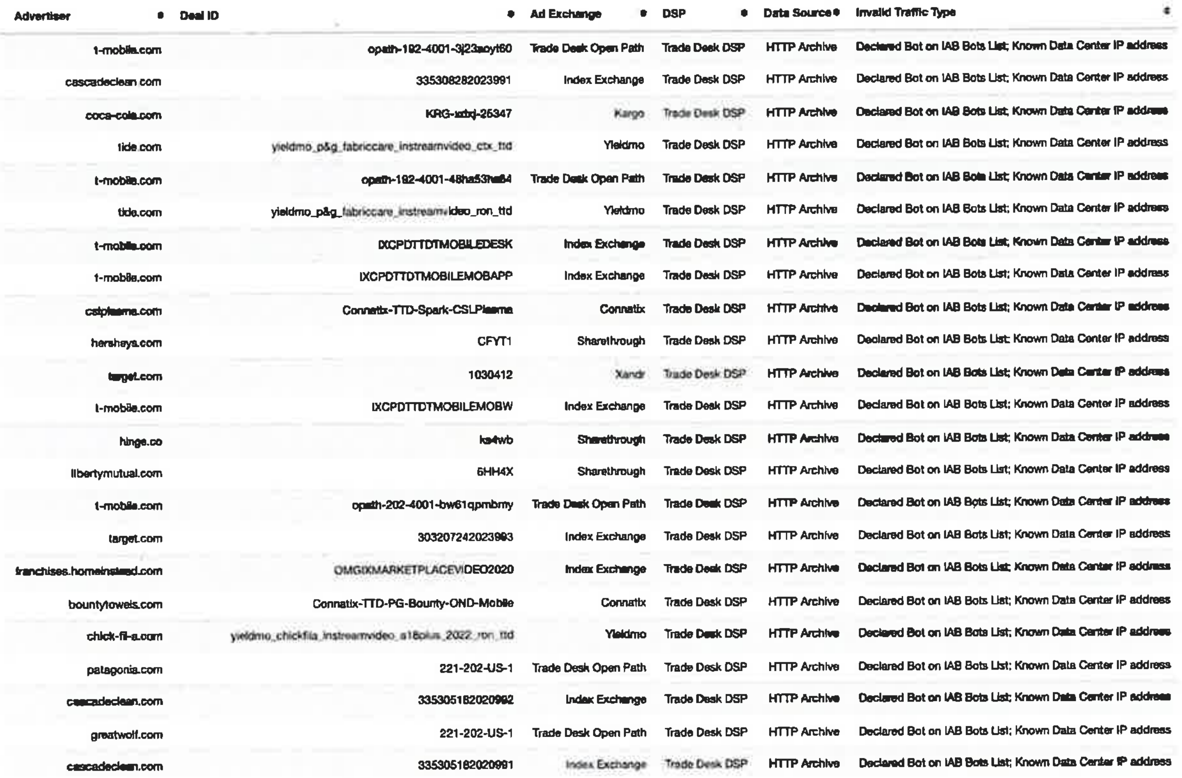
Table illustrating via which PMP deals Hershey's ads were served to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP

As a fifth example, T-Mobile had ads served to declared bots operating out of data center IPs by Index Exchange, Microsoft Xandr, ShareThrough, Connatix, Kargo, OpenX, Google, and Trade Desk Open Path. The T-Mobile ads served to bots via Index Exchange were transacted via PMP deals IDs IXCPDTTDTMOBILEDESK, IXCPDTTDTMOBILEMOBAPP, IXCPDTTDTMOBILEOUT, and others; the T-Mobile ads served to bots via Kargo were transacted via PMP deal IDs KRG-lhgk-27510, KRG-vkt1-27511, and KRG-78wk-27512, the T-Mobile ads served to bots via Connatix were transacted via PMP deal IDs Connatix-TTD-TMobile-RON-Desktop and Connatix-TTD-TMobile-RON-Mobile; the T-Mobile ads served to bots via ShareThrough were transacted via PMP deal ID 1zzwD.



Advertiser	Deal ID	Ad Exchange	DSP	Data Source	Invalid Traffic Type
t-mobile.com	1zzwD	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	1439277	Xandr	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	1439280	Xandr	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	9311192021991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	9311192021992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	549644398141615063	Google	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	549644398141764286	Google	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	Connatix-TTD-TMobile-RON-Desktop	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	Connatix-TTD-TMobile-RON-Mobile	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEDESK	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEMOBAPP	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEMOBW	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEOUT	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEVID	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	KRG-78wk-27512	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	KRG-lhgk-27510	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	KRG-vkt1-27511	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-192-4001-3j23aoy160	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-192-4001-48ha53ha64	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-202-4001-82coeyei2u	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-202-4001-bw81qpmbmy	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-202-4001-r0ygm500ex	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address

Table illustrating via which PMP deals T-Mobile ads were served to a declared bot (whose user agent is on the IAB Tech Lab Spiders and Bots list since 2013) operating out of well known data center IP



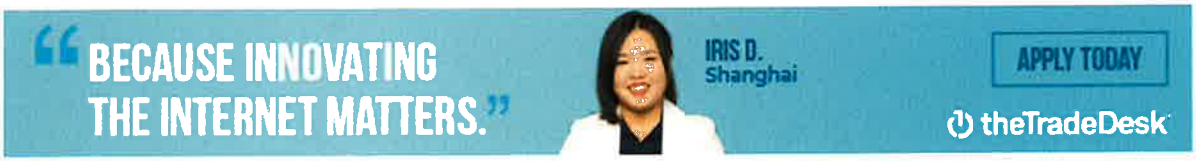
Advertiser	Deal ID	Ad Exchange	DSP	Data Source	Invalid Traffic Type
t-mobile.com	opath-192-4001-3j23aoyt60	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335308282023991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
coca-cola.com	KRG-xdxj-25347	Kargo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_instreamvideo_ctx_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-192-4001-48ha53ha84	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
tide.com	yieldmo_p&g_fabriccare_instreamvideo_ron_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEDESK	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEMOBAPP	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cslplasma.com	Connatix-TTD-Spark-CSLPlasma	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hersheys.com	CFYT1	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
target.com	1030412	Xandr	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	IXCPDTTDTMOBILEMOBW	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
hinge.co	ks4wb	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
libertymutual.com	6HH4X	Sharethrough	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
t-mobile.com	opath-202-4001-bw61qpmbmy	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
target.com	303207242023993	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
franchises.homeinstead.com	OMGIXMARKETPLACEVIDEO2020	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
bountytowels.com	Connatix-TTD-PG-Bounty-OND-Mobile	Connatix	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
chick-fil-a.com	yieldmo_chickfila_instreamvideo_a18plus_2022_ron_ttd	Yieldmo	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
patagonia.com	221-202-US-1	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020992	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
greatwolf.com	221-202-US-1	Trade Desk Open Path	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address
cascadeclean.com	335305182020991	Index Exchange	Trade Desk DSP	HTTP Archive	Declared Bot on IAB Bots List; Known Data Center IP address

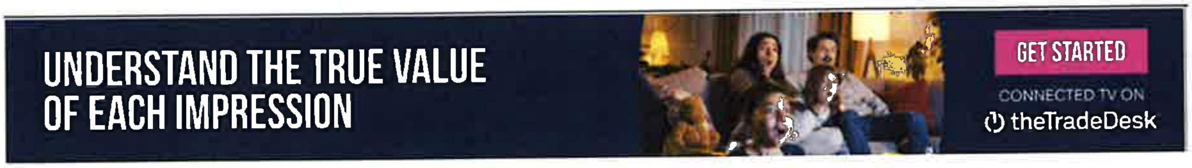
Data table showing a sample of brands whose ads were served to declared bot in data center server farms, wherein the ad appears to have been mediated via a private marketplace or other type of deal ID.

Ads promoting the Trade Desk itself - in its capacity as an advertiser - served to bots by Trade Desk and other vendors that claim to partner with HUMAN Security

The Trade Desk was observed running ads on various websites promoting its own product and services.

For example, in the screenshots below, one can see a few examples of Trade Desk ad creatives. The first ad appears to be a job recruiting ad, soliciting applications to work for the Trade Desk. The second ad appears to be promoting Trade Desk's connected television offerings.



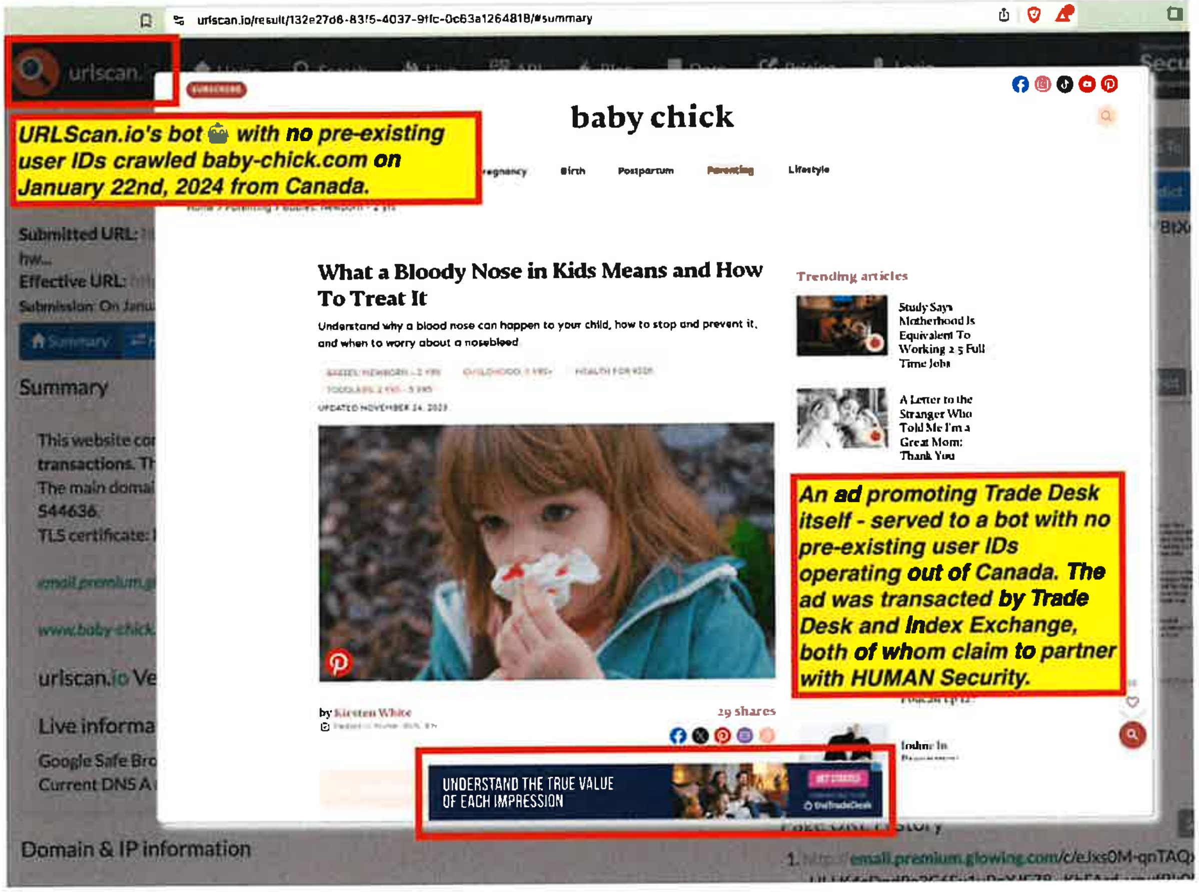


YOU'RE SEEING THIS AD
BECAUSE JOURNALISM MATTERS
LEARN MORE
theTradeDesk

Trade Desk was observed serving its own job recruiting and product marketing ads to bots over the course of several years.

For example, in the screenshot below, one can see a Trade Desk ad that says: "UNDERSTAND THE TRUE VALUE OF EACH IMPRESSION" served to URLScan.io's bot whilst the bot was crawling baby-chick.com on January 22nd, 2024. The Trade Desk ad was served to the bot by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security.

https://adalytics.io/blog/prebid-bot-filtration



URLScan.io's bot 🤖 with no pre-existing user IDs crawled baby-chick.com on January 22nd, 2024 from Canada.

What a Bloody Nose in Kids Means and How To Treat It

Understand why a blood nose can happen to your child, how to stop and prevent it, and when to worry about a nosebleed

Trending articles

Study Says Motherhood Is Equivalent To Working 2.5 Full Time Jobs

A Letter to the Stranger Who Told Me I'm a Great Mom: Thank You

An ad promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating out of Canada. The ad was transacted by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security.

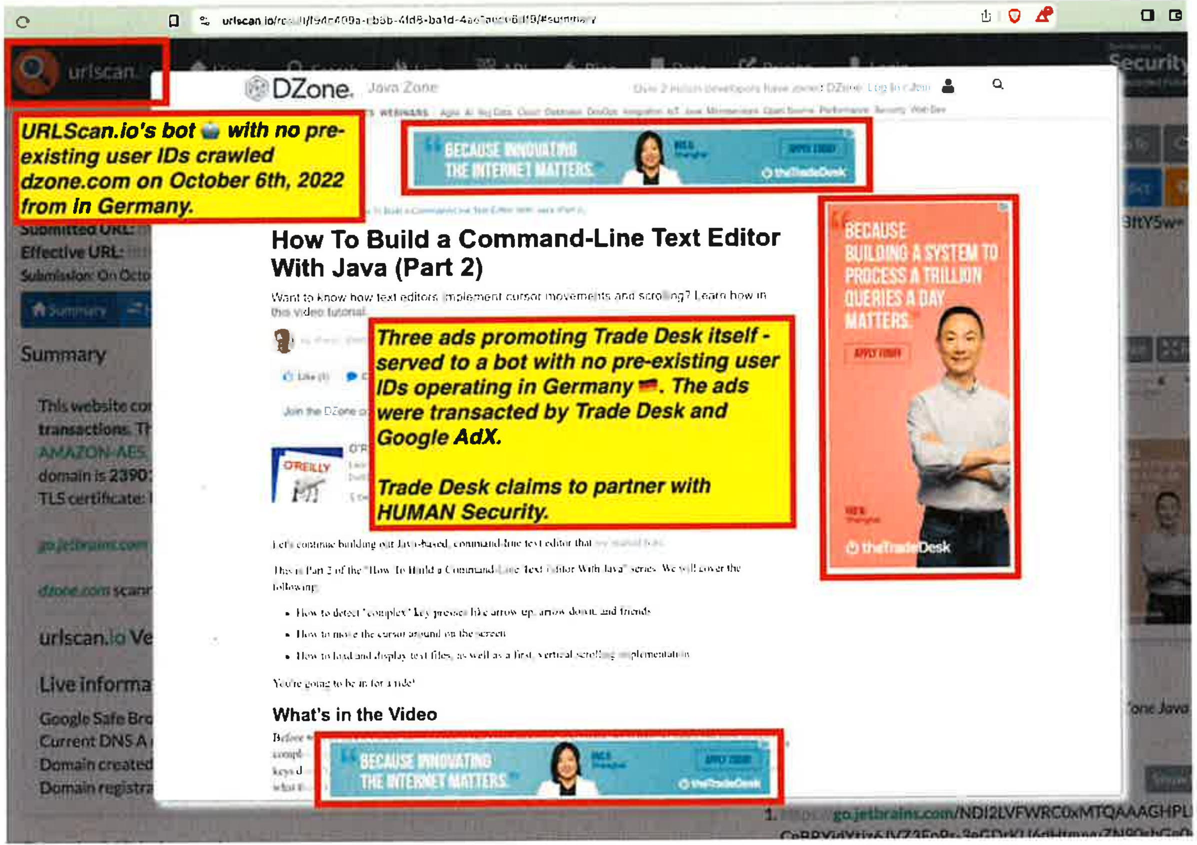
by Kirsten White

29 shares

A Trade Desk ad that says: "UNDERSTAND THE TRUE VALUE OF EACH IMPRESSION" served to URLScan.io's bot whilst the bot was crawling baby-chick.com on January 22nd, 2024. The Trade Desk ad was served to the bot by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security. Source: https://urlscan.io/result/132e27d6-83f5-4037-9ffc-0c63a1264818/#summary

As another example, in the screenshot below, one can see three Trade Desk job recruiting ads that were served to URLScan.io's bot whilst the bot was crawling dzone.com on October 6th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Google AdX.

https://adalytics.io/blog/prebid-bot-filtration


urlscan
DZone. Java Zone
BECAUSE INNOVATING THE INTERNET MATTERS.
theTradeDesk
BECAUSE BUILDING A SYSTEM TO PROCESS A TRILLION QUERIES A DAY MATTERS.
APPLY TODAY
Summary
O'REILLY
1. go.jetbrains.com/NDI2LVFWRC0xMTQAAAGHPL

URLScan.io's bot 🤖 with no pre-existing user IDs crawled dzone.com on October 6th, 2022 from in Germany.

Three ads promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating in Germany 🇩🇪. The ads were transacted by Trade Desk and Google AdX.

Trade Desk claims to partner with HUMAN Security.

How To Build a Command-Line Text Editor With Java (Part 2)

Want to know how text editors implement cursor movements and scrolling? Learn how in this video tutorial.

Let's continue building our Java-based, command-line text editor that

This is Part 2 of the "How To Build a Command-Line Text Editor With Java" series. We will cover the following:

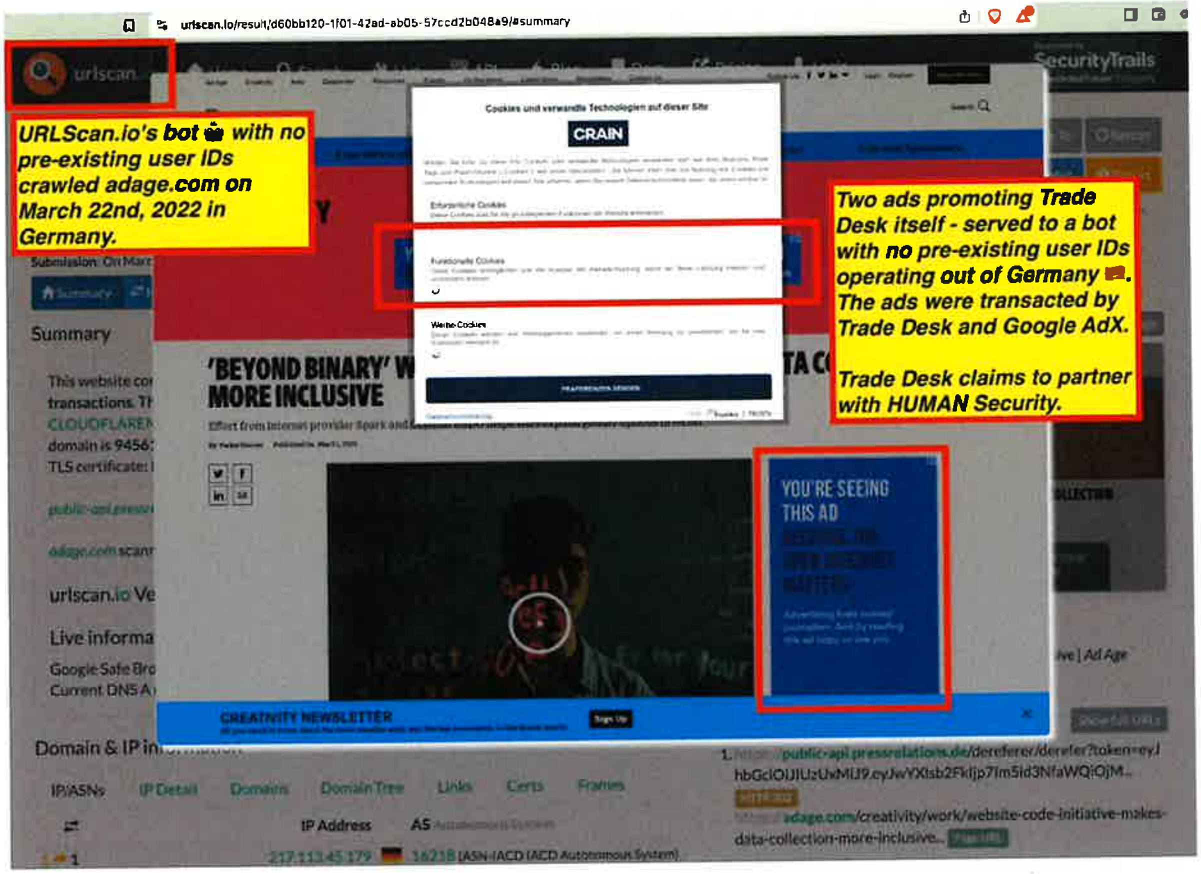
- How to detect "complex" key presses like arrow up, arrow down, and friends
- How to move the cursor around on the screen
- How to load and display text files, as well as a first, vertical scrolling implementation

You're going to be in for a ride!

What's in the Video

Three Trade Desk job recruiting ads that were served to URLScan.io's bot whilst the bot was crawling dzone.com on October 6th, 2022. The Trade Desk ad was served to the bot by Trade Desk and Google AdX. Source: https://urlscan.io/result/f94c409a-cb5b-4fd8-ba1d-4ae1aece6df9/#summary

As another example, in the screenshot below, one can see two Trade Desk ads that were served to URLScan.io's bot whilst the bot was crawling adage.com on March 22nd, 2022. The Trade Desk ads were served to the bot by Trade Desk and Google AdX.



urlscan.io/result/d60bb120-1f01-42ad-ab05-57ccd2b048a9/#summary

URLScan.io's bot 🤖 with no pre-existing user IDs crawled adage.com on March 22nd, 2022 in Germany.

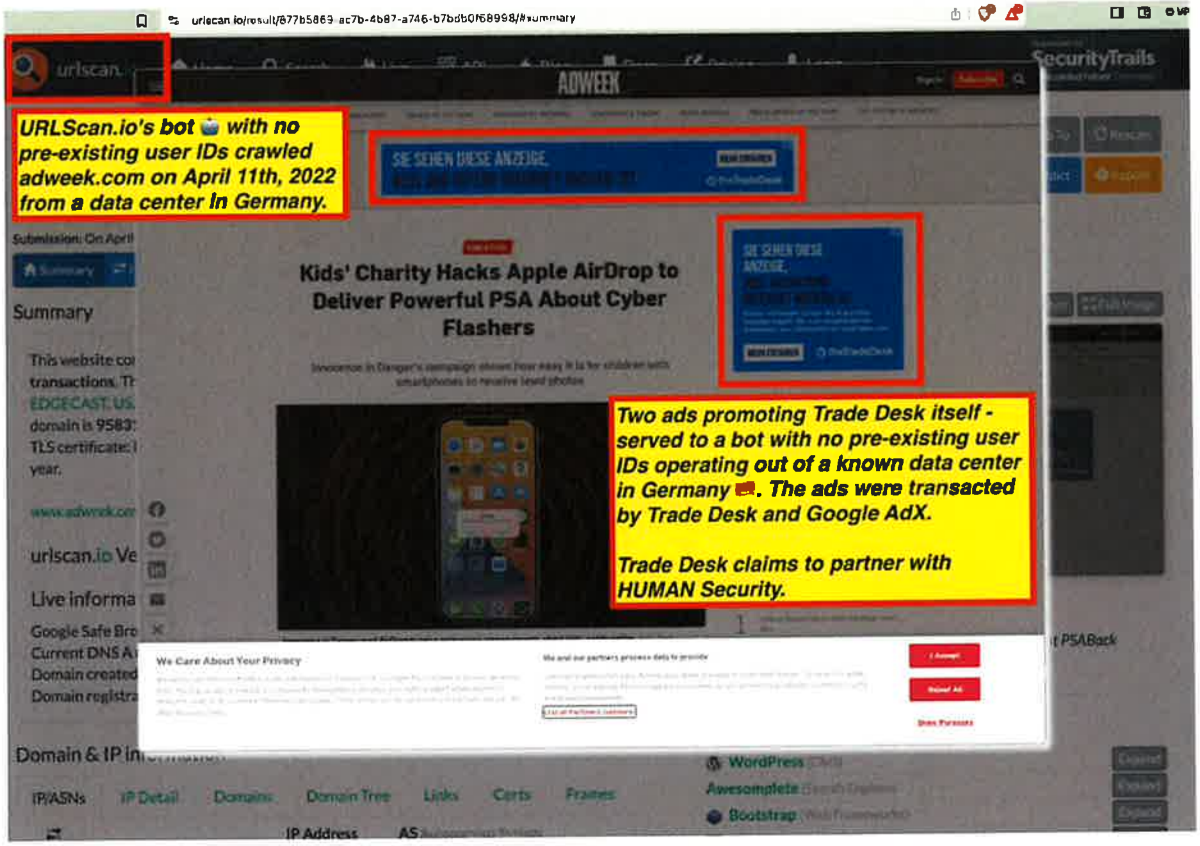
Two ads promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating out of Germany 🇩🇪. The ads were transacted by Trade Desk and Google AdX.

Trade Desk claims to partner with HUMAN Security.

urlscan
SecurityTrails
Cookies und verwandte Technologien auf dieser Site
CRAIN
'BEYOND BINARY' W
MORE INCLUSIVE
YOU'RE SEEING THIS AD
CREATIVITY NEWSLETTER
Sign Up
Summary
urlscan.io Ve
Live informa
Domain & IP in
IP/ASNs
IP Detail
Domains
Domain Tree
Links
Certs
Frames
IP Address
AS
217.113.45.179
16218 (ASN-IACD (ACD Autonomous System)
public-api.pressrelations.de/dereferer/dereferer?token=eyJ
adage.com/creativity/work/website-code-initiative-makes-data-collection-more-inclusive...

As another example, in the screenshot below, one can see two Trade Desk ads that were served to URLScan.io's bot whilst the bot was crawling adage.com on March 22nd, 2022. The Trade Desk ads were served to the bot by Trade Desk and Google AdX. Source: https://urlscan.io/result/d60bb120-1f01-42ad-ab05-57ccd2b048a9/#summary

As another example, in the screenshot below, one can see two Trade Desk ads that were served to URLScan.io's bot whilst the bot was crawling adweek.com on April 11th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Google AdX.



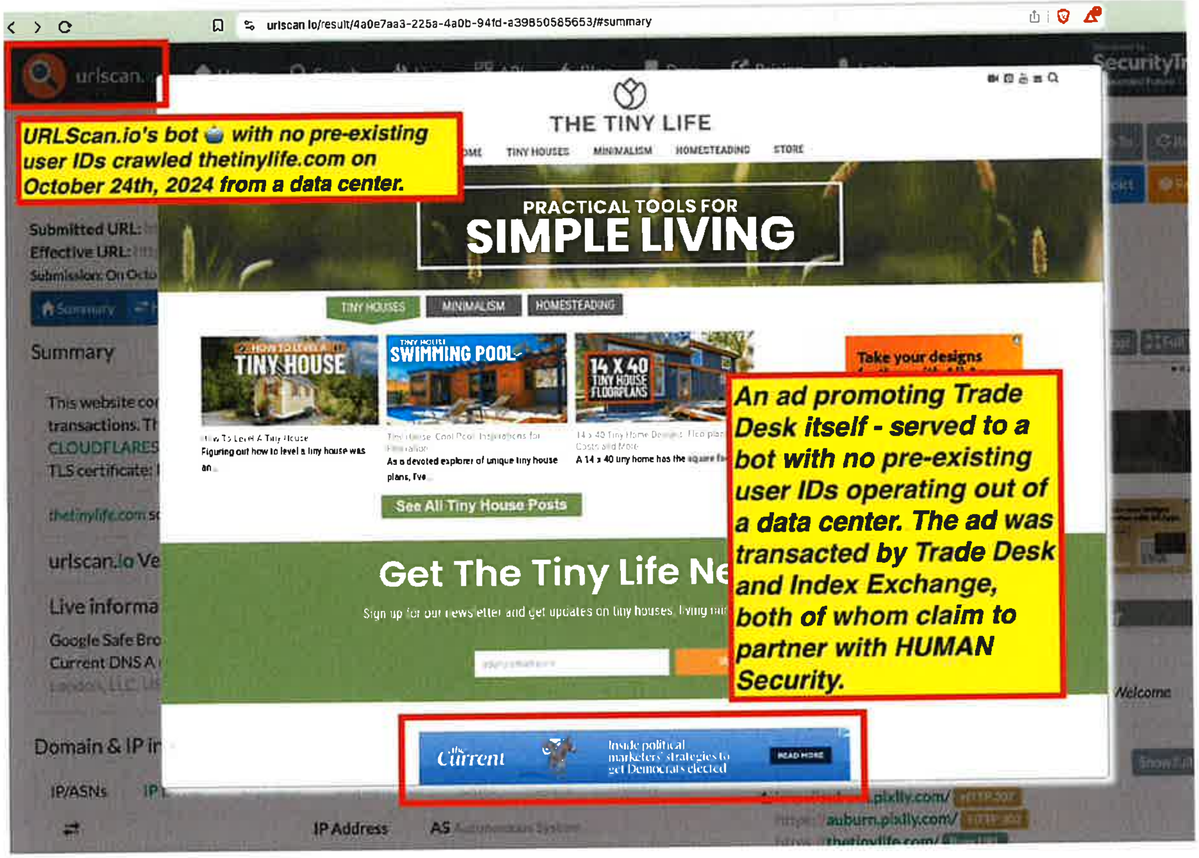
URLScan.io's bot 🤖 with no pre-existing user IDs crawled adweek.com on April 11th, 2022 from a data center in Germany.

Two ads promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating out of a known data center in Germany 🇩🇪. The ads were transacted by Trade Desk and Google AdX.

Trade Desk claims to partner with HUMAN Security.

As another example, in the screenshot below, one can see two Trade Desk ads that were served to URLScan.io's bot whilst the bot was crawling adweek.com on April 11th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Google AdX. Source: https://urlscan.io/result/877b5869-ac7b-4b87-a746-b7bdb0f68998/#summary

As another example, in the screenshot below, one can see a Trade Desk ad that says: "Inside political marketers' strategies to get Democrats elected" that was served to URLScan.io's bot whilst the bot was crawling thetinylife.com on October 24th, 2024. The Trade Desk ads were served to the bot by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security.

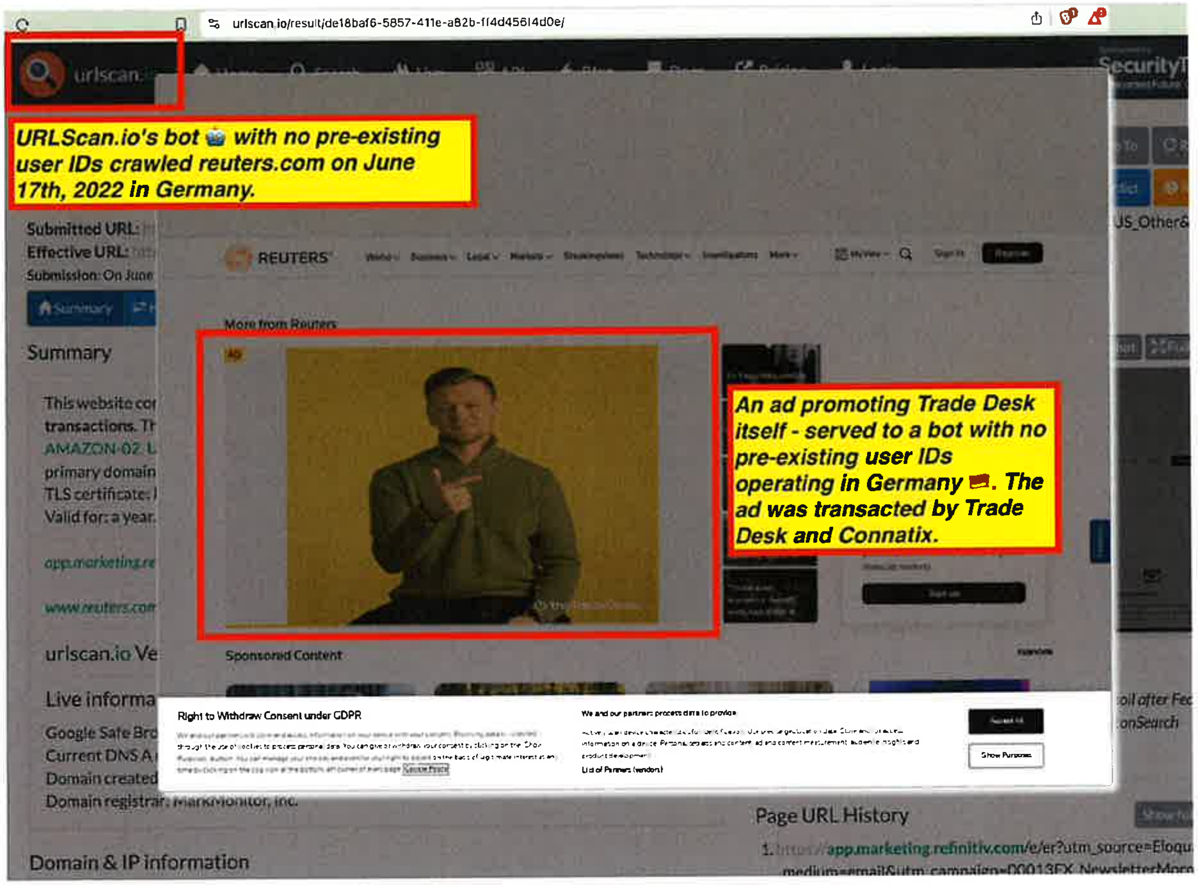


URLScan.io's bot 🤖 with no pre-existing user IDs crawled thetinylife.com on October 24th, 2024 from a data center.

An ad promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating out of a data center. The ad was transacted by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security.

A Trade Desk ad that says: "Inside political marketers' strategies to get Democrats elected" that was served to URLScan.io's bot whilst the bot was crawling thetinylife.com on October 24th, 2024. The Trade Desk ads were served to the bot by Trade Desk and Index Exchange, both of whom claim to partner with HUMAN Security. Source: https://urlscan.io/result/4a0e7aa3-225a-4a0b-94fd-a39850585653/#summary

As another example, in the screenshot below, one can see a Trade Desk video ad that was served to URLScan.io's bot whilst the bot was crawling reuters.com.com on June 17th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Connatix.


urlscan.io/result/de18baf6-5857-411e-a82b-ff4d456f4d0e/

URLScan.io's bot 🤖 with no pre-existing user IDs crawled reuters.com on June 17th, 2022 in Germany.

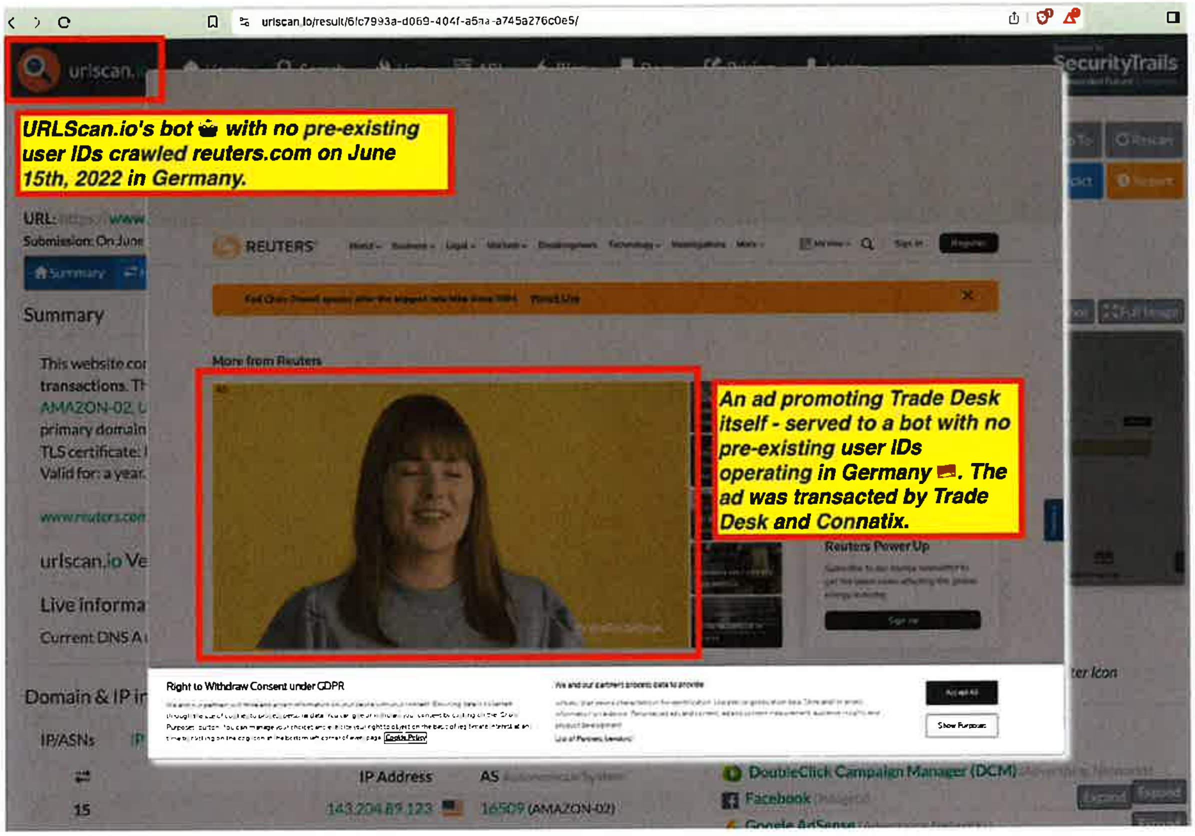
An ad promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating in Germany 🇩🇪. The ad was transacted by Trade Desk and Connatix.

Page URL History

1. https://app.marketing.refinitiv.com/e/er?utm_source=Eloqu medium=email&utm_campaign=00013FX NewsletterMore

A Trade Desk video ad that was served to URLScan.io's bot whilst the bot was crawling reuters.com.com on June 17th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Connatix. Source: https://urlscan.io/result/de18baf6-5857-411e-a82b-ff4d456f4d0e/#summary

As another example, in the screenshot below, one can see a Trade Desk video ad that was served to URLScan.io's bot whilst the bot was crawling reuters.com.com on June 15th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Connatix.



urlscan.io/result/6fc7993a-d069-404f-a5aa-a745a276c0e5/

URLScan.io's bot 🤖 with no pre-existing user IDs crawled reuters.com on June 15th, 2022 in Germany.

An ad promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating in Germany 🇩🇪. The ad was transacted by Trade Desk and Connatix.

A Trade Desk video ad that was served to URLScan.io's bot whilst the bot was crawling reuters.com.com on June 15th, 2022. The Trade Desk ads were served to the bot by Trade Desk and Connatix. Source: https://urlscan.io/result/6fc7993a-d069-404f-a5aa-a745a276c0e5/#summary

Research Results: Brands whose ads include references to "charge-allDoubleVerifyBotAvoidance" and had their ads served to bots

Hundreds of major brands whose ads' source code include references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify appear to have had their ads served to bots in data centers.

Firstly, many brands whose ads' source includes references to "charge-allDoubleVerifyBotAvoidance" had their ads served to declared bots operating out of well known data center IP addresses. The brands had their ads served to the HTTP Archive bot, whose user agent has been on the IAB Tech Lab Spiders and Bots reference list since 2013. The IP addresses of data centers used by the HTTP Archive are well known, publicized Google Cloud data center IPs.

For example, the United States Navy had ads served over the course of several years to declared bots on the IAB Bots List operating out of known data center IPs, wherein the US Navy ads' source code included references to "charge-allDoubleVerifyBotAvoidance". For example, the US Navy had its ads served to a declared bot operating out of a known data center IP in September 2022 on the website infectious-smile.fandom.com. The US Navy ad was transacted by the SSP Kargo, via Kargo PMP deal ID KRG-2pwj-22414. Kargo SSP also partners with HUMAN Security for bot mitigation. The US Navy also had ads served via Index Exchange, Microsoft Xandr, and the Media Grid to declared bots on the IAB Bots List operating out of known data center IPs, wherein the US Navy ads' source code included references to "charge-allDoubleVerifyBotAvoidance".

As a second example, Pfizer had paxlovid.com ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the Pfizer ads' source code included references to "charge-allDoubleVerifyBotAvoidance". For example, in November 2023, Pfizer had its paxlovid.com ads served to a declared bot operating out of a known data center IP whilst the HTTP Archive bot was crawling the website testsworld.net.

As a third example, the Government of DC had dchealth.dc.gov ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the DC Government ads' source code included references to "charge-allDoubleVerifyBotAvoidance". For example, in August 2022, the DC Government had its dchealth.gov ads served to a declared bot operating out of a known data center IP whilst the HTTP Archive bot was crawling the website selonpepite.canalblog.com.

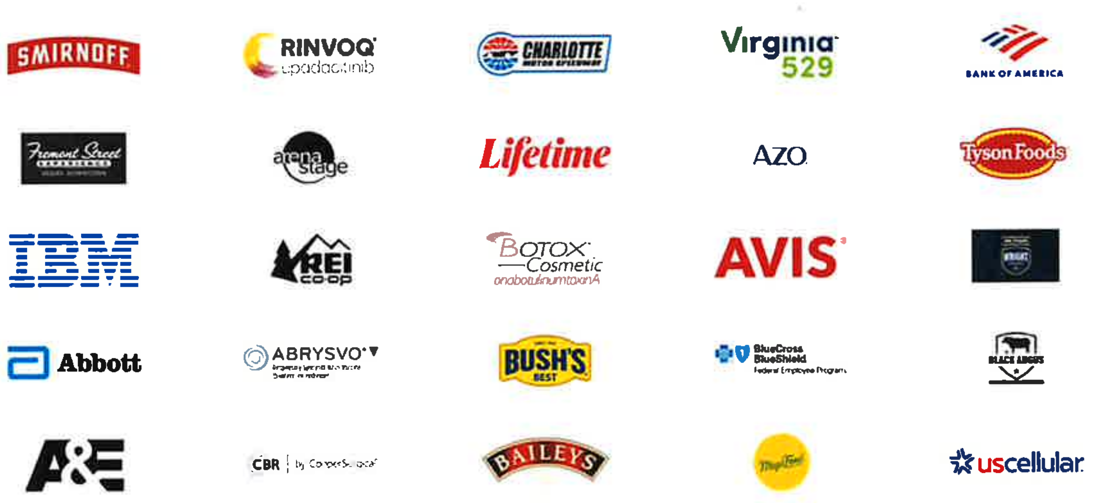
As a fourth example, Haleon had advil.com ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the Haleon ads' source code included references to "charge-allDoubleVerifyBotAvoidance". For example, in March 2024, Haleon had its advil.com ads served to a declared bot operating out of a known data center IP whilst the HTTP Archive bot was crawling the website cinderella-phenomenon.fandom.com.

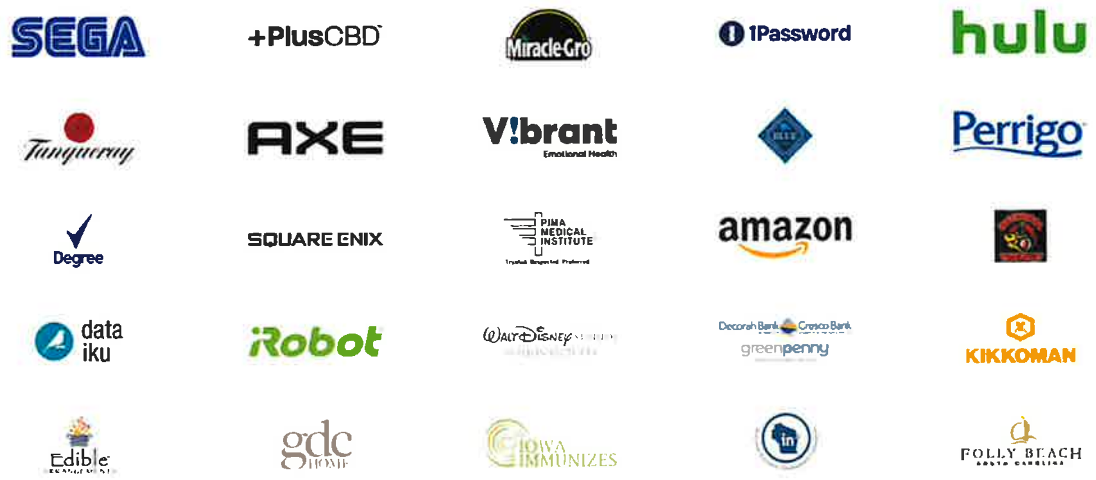
The list of brands whose ads' source code includes references to "charge-allDoubleVerifyBotAvoidance", and had their ads served to a declared bot on the IAB Bots List operating out of a known data center IP address included many major brands such as the United States Navy, the Government of the State of New York, the Government of Singapore, Ernst & Young (EY), IBM, Unilever, Bank of America, Adobe, McCormick & Company, Tyson Foods, Wawa, US Cellular, Jimmy Dean, Ozempic (owned by Novo Nordisk), Abbott, T. Rowe Price, Lexus, Abbvie, American Eagle, Chick-fil-A, US Bank, Amazon, Edward Jones, Vauxhall Motors, Subaru, Amgen, Aveva, Loccitane, Ticketmaster, Diageo, Asus, Michelin tire company, Kia, Orkin, Siemens Healthineers, Survey Monkey, Disabled American Veterans (dav.org), Intuit, Panera Bread, CBS Interactive, 1password, Anti-Defamation League (adl.org), AMC Theaters, BMW USA, Paxlovid (owned by Pfizer), Vanguard, Arexvy (owned by GlaxoSmithKline or GSK), Salix Pharmaceuticals, and many others.

Brands whose ads referenced "charge-allDoubleVerifyBotAvoidance" & were served to declared bots (listed on the IAB Bots & Spiders List since 2013) operating from known data center IPs

Wawa
Chick-fil-A
unicef
usbank
STOP HIV IOWA
SUBARU
Pfizer
HOME CHEF
OZEMPIC
NAVY
Whirlpool
GLASSDOOR
Dove
Direxion
COMIRNATY
TARGET
RESERVEBAR
GAILLARD
STEINBERG
Jimmy Dean
STEEN ENTERPRISES
DOORDASH
MethylLife

https://adalytics.io/blog/prebid-bot-filtration





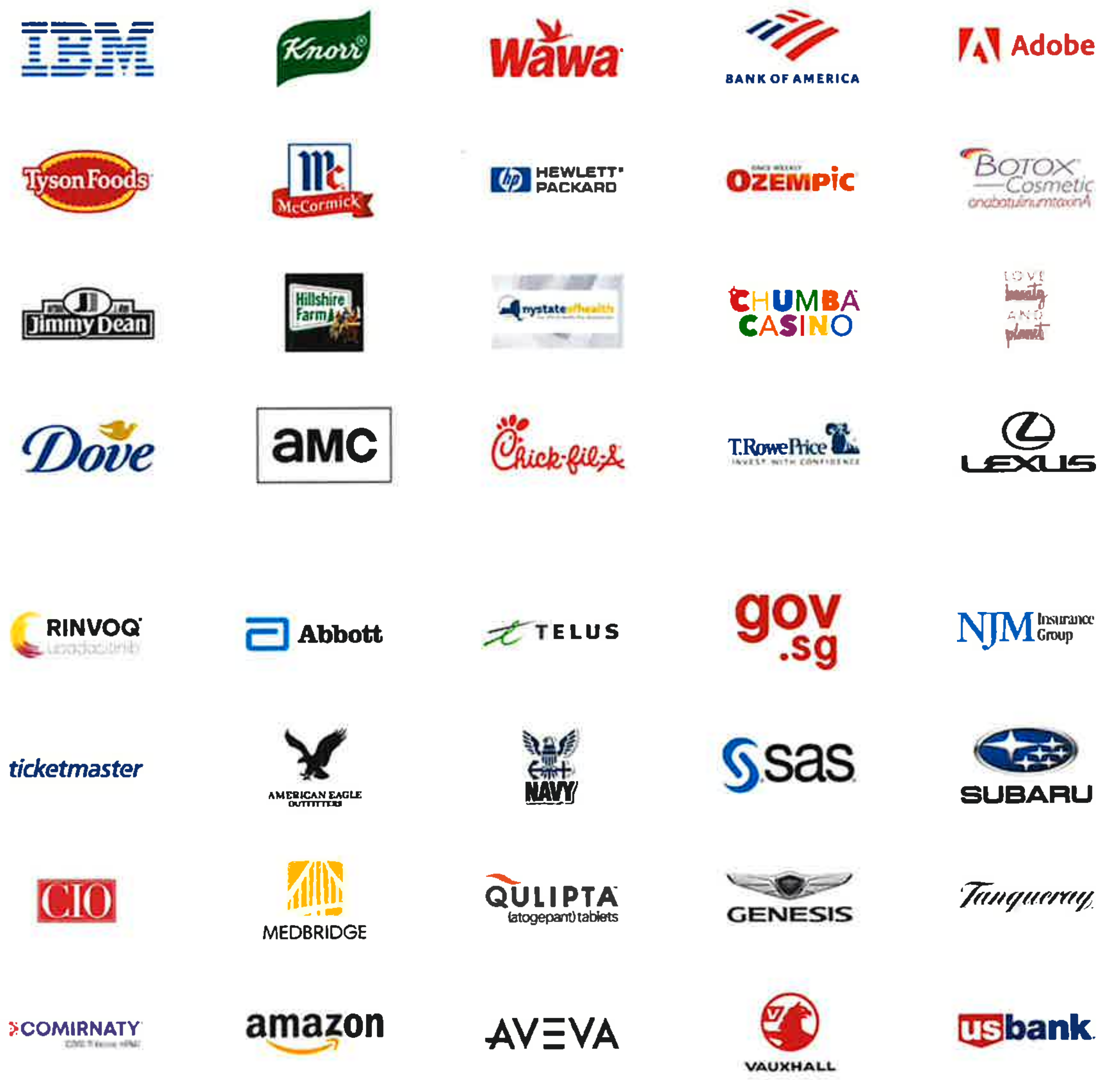
On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

WOMEN UNITED
Southwest
RYBELSUS semaglutide tablets
United Healthcare
HAZELCAST
ticketmaster
SHOWTIME
Scotts
Vanguard
Ball Park
NW NORTHWEST FEDERAL CREDIT UNION
Book Outlet
Boar's Head
BIG LOTS!
Benlysta
azstarys
CIBINQO
ASCENT
Advil
Adobe
ACURA
abbvie
A24
CHEVROLET
Carnegie Mellon University

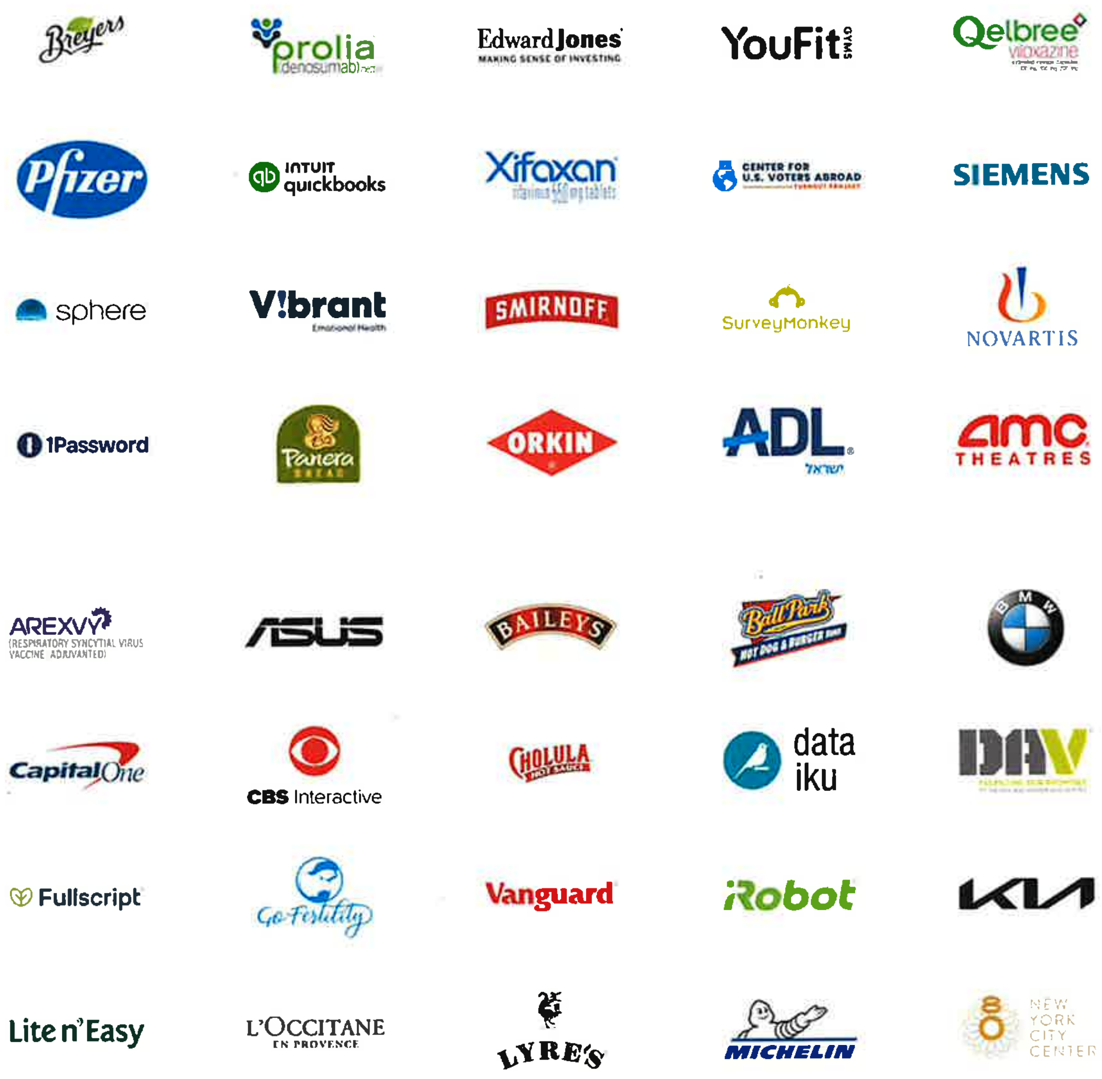
Kroger
OLLY
NAVY FEDERAL Credit Union
ARMY
MARINE CORPS
NAVY
AIR FORCE
COAST GUARD
SPACE FORCE
VETERANS
MAYO CLINIC
LAS VEGAS MOTOR SPEEDWAY
Shriners Hospitals for Children
Love to the rescue
40 YEARS Lexia
Knorr
GENESIS
KLONDIKE
INTERNATIONAL POVERTY FORUM
INKBOX
IKON PASS
HISTORY
HELLMANN'S
EST.1913
Carnegie Mellon University

https://adalytics.io/blog/prebid-bot-filtration

Brands whose ads referenced "charge-allDoubleVerifyBotAvoidance" & were served to URLScan.io bots



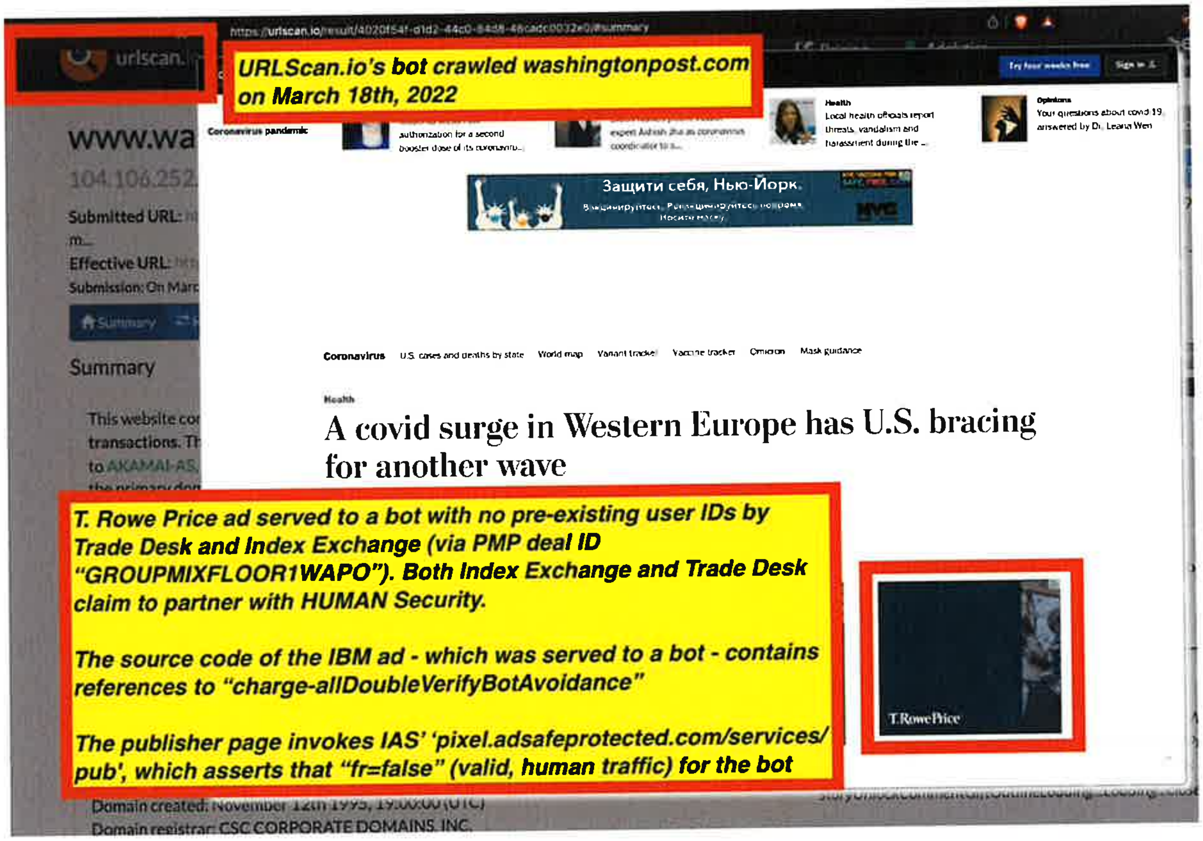
[On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?](https://adalytics.io/blog/prebid-bot-filtration)



Furthermore, many brands whose ads appear to contain code from DoubleVerify and whose source code references "charge-allDoubleVerifyBotAvoidance" appear to have had their ads served to URLScan.io's bot when the bot was crawling various websites with no pre-existing user IDs.

For example, in the screenshot below, one can see an instance where a T. Rowe Price ad was served to URLScan.io's bot whilst the bot was crawling washingtonpost.com on March 18th, 2022. The T. Rowe Price ad was transacted by GroupM, Trade Desk, and Index Exchange (via PMP deal ID "GROUPMIXFLOOR1WAPO"). The source code of the T.

Rowe Price ad that was served to URLScan.io's bot includes source code from DoubleVerify and references to "charge-allDoubleVerifyBotAvoidance".



URLScan.io's **bot crawled washingtonpost.com** on **March 18th, 2022**

T. Rowe Price ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "GROUPMIXFLOOR1WAPO"). Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

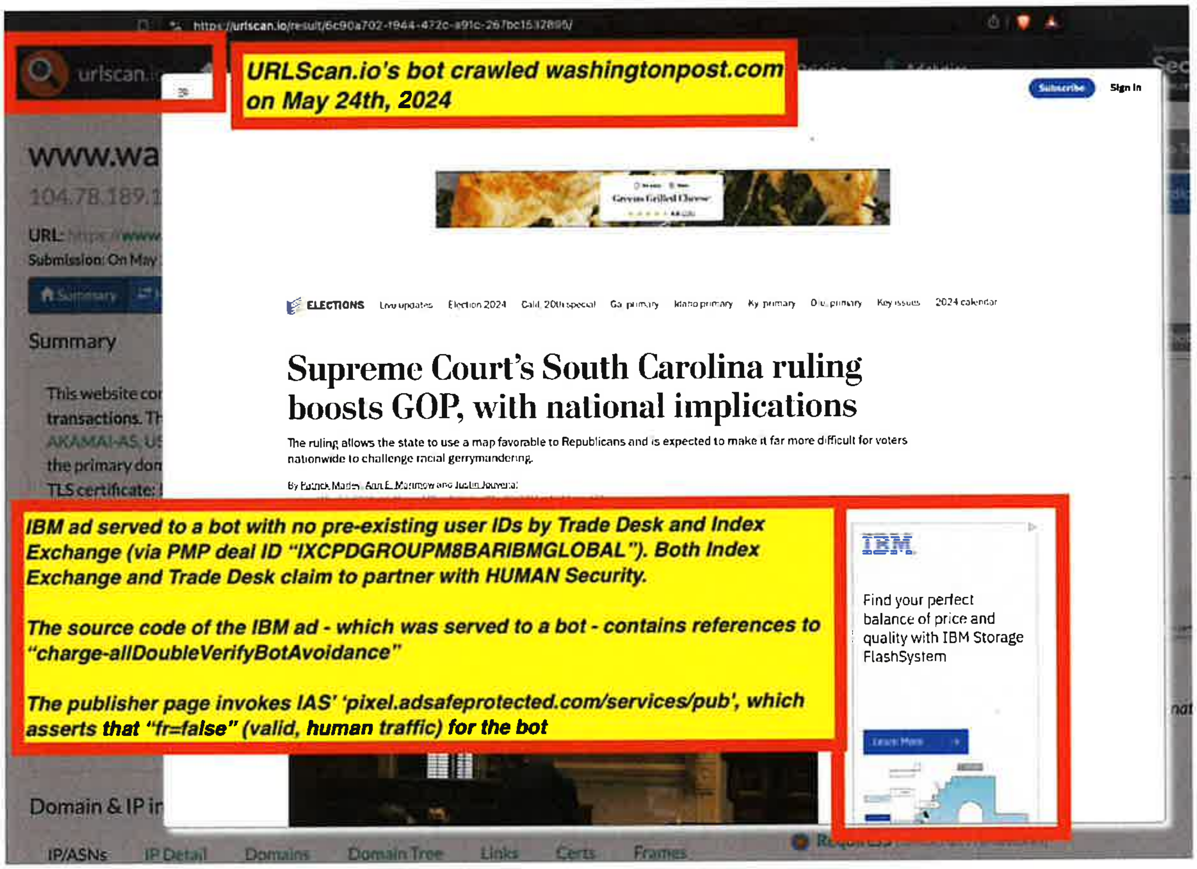
The source code of the IBM ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

The publisher page invokes IAS' 'pixel.adsafeprotected.com/services/pub', which asserts that "fr=false" (valid, **human traffic) for the bot**

https://urlscan.io/result/4020f54f-d1d2-44c0-84d8-46cadc0032e0/#summary
urlscan.
www.wa
104.106.252.
Submitted URL:
Effective URL:
Submission: On Marc
Summary
This website co
transactions. T
to AKAMAI-AS,
Coronavirus pandemic
Health
Local health officials report threats, vandalism and harassment during the ...
Opinions
Your questions about covid 19 answered by Dr. Leana Wen
Защити себя, Нью-Йорк.
Coronavirus
U.S. cases and deaths by state
World map
Variant tracker
Vaccine tracker
Omicron
Mask guidance
Health
A covid surge in Western Europe has U.S. bracing for another wave
T.RowePrice
Domain created: November 12th 1995, 19:00:00 (UTC)
Domain registrar: CSC CORPORATE DOMAINS, INC.

Screenshot of a T. Rowe Price ad served to URLScan.io's bot and transacted by GroupM, Trade Desk, and Index Exchange. The source code of the T. Rowe Price ad includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/4020f54f-d1d2-44c0-84d8-46cadc0032e0/

As another example, in the screenshot below, one can see an instance where an IBM ad was served to URLScan.io's bot whilst the bot was crawling washingtonpost.com on May 24th, 2024. The IBM ad was transacted by GroupM, Trade Desk, and Index Exchange (via PMP deal ID "IXCPDGROUPM8BARIMGLOBAL"). The source code of the IBM ad that was served to URLScan.io's bot includes source code from DoubleVerify and references to "charge-allDoubleVerifyBotAvoidance".



URLScan.io's bot crawled washingtonpost.com on May 24th, 2024

ELECTIONS Live updates Election 2024 Calif. 20th special Ga. primary Idaho primary Ky. primary Ore. primary Key issues 2024 calendar

Supreme Court's South Carolina ruling boosts GOP, with national implications

The ruling allows the state to use a map favorable to Republicans and is expected to make it far more difficult for voters nationwide to challenge racial gerrymandering.

By Patrick Marley, Ann E. Marimow and Justin Jouvenal

IBM ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange (via PMP deal ID "IXCPDGROUPM8BARIBMGLOBAL"). Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

The source code of the IBM ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

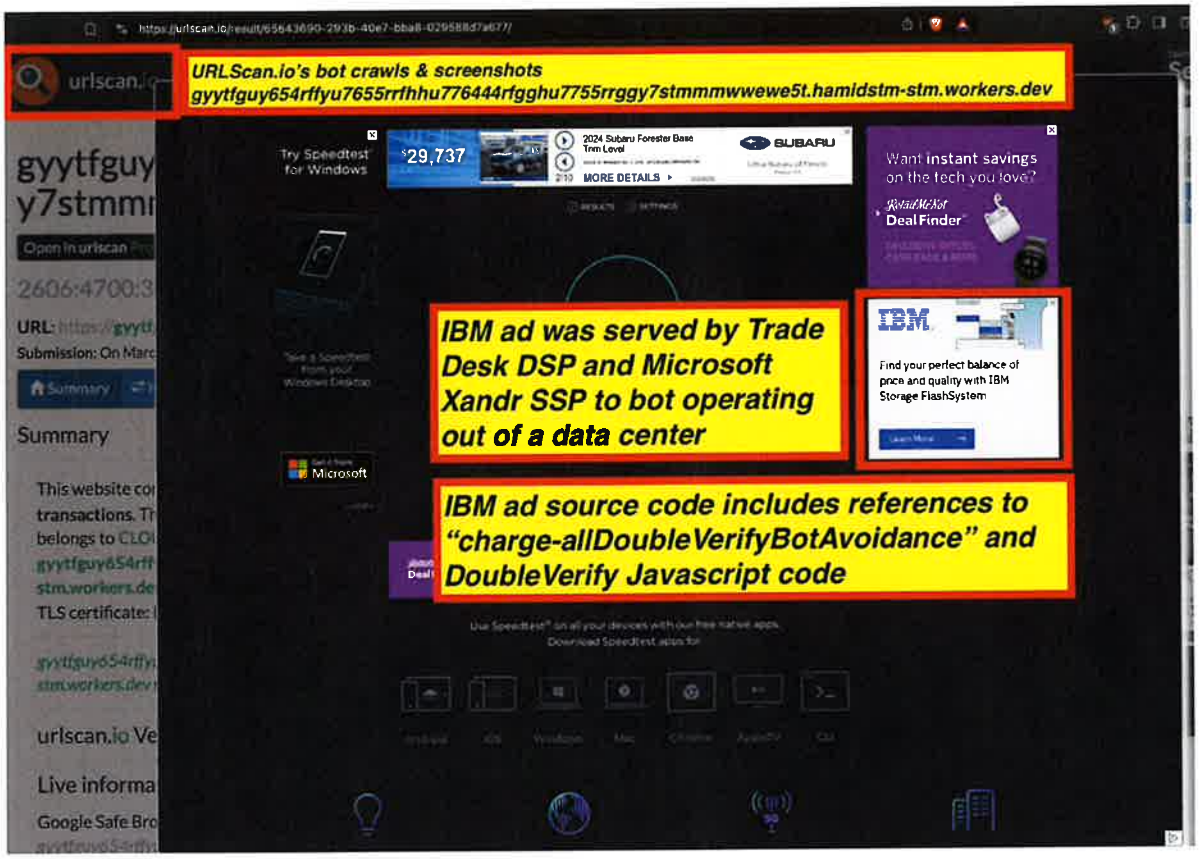
The publisher page invokes IAS' 'pixel.adsafeprotected.com/services/pub', which asserts that "fr=false" (valid, human traffic) for the bot

IBM

Find your perfect balance of price and quality with IBM Storage FlashSystem

Screenshot of an IBM ad served to URLScan.io's bot and transacted by GroupM, Trade Desk, and Index Exchange. The source code of the IBM ad includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/6c90a702-f944-472c-a91c-267bc1532895/

As another example, in the screenshot below, one can see an instance where an IBM ad was served to URLScan.io's bot whilst the bot was crawling gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev on March 12th, 2024. The IBM ad was transacted by GroupM, Trade Desk, and Microsoft Xandr (via PMP deal ID "IXCPDGROUPM8BARIMGLOBAL"). The source code of the IBM ad that was served to URLScan.io's bot with no pre-existing user IDs includes source code from DoubleVerify and references to "charge-allDoubleVerifyBotAvoidance".



URLScan.io's bot crawls & screenshots gyytfguy654rffyu7655rrfhhu776444rfgghu7755rrggy7stmmmwwewe5t.hamidstm-stm.workers.dev

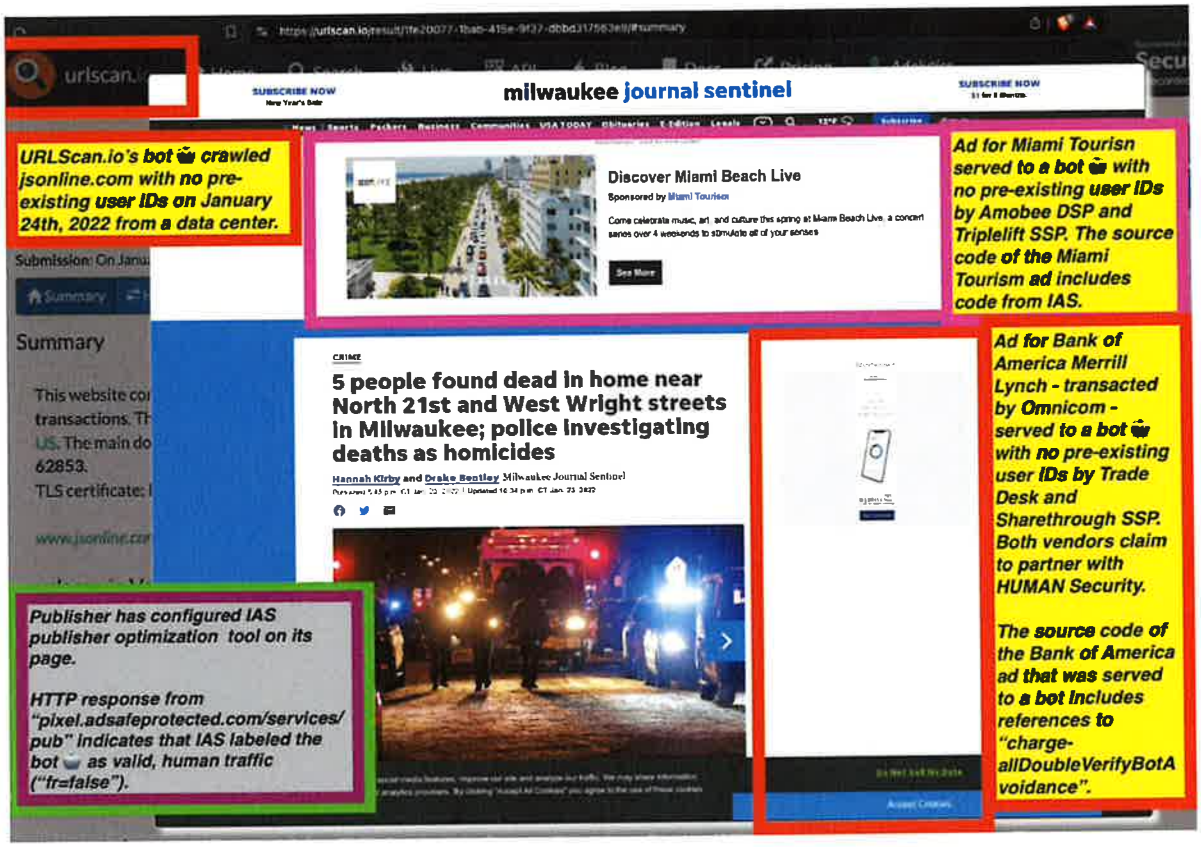
IBM ad was served by Trade Desk DSP and Microsoft Xandr SSP to bot operating out of a data center

IBM ad source code includes references to "charge-allDoubleVerifyBotAvoidance" and DoubleVerify Javascript code

Screenshot of an IBM ad served to URLScan.io's bot and transacted by GroupM, Trade Desk, and Microsoft Xandr SSP. The source code of the IBM ad includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/65643690-293b-40e7-bba8-029588d7a677/

As another example, a Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling jsonline.com on January 24th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Sharethrough, all three of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".

The publisher jsonline.com appears to have configured IAS' publisher optimization tool on its page. The IAS tool appears to have classified the URLScan.io bot as "fr=false" (valid, human traffic).



URLScan.io's bot 🤖 crawled jsonline.com with no pre-existing user IDs on January 24th, 2022 from a data center.

Discover Miami Beach Live

Sponsored by Miami Tourism

Come celebrate music, art, and culture this spring at Miami Beach Live, a concert series over 4 weekends to stimulate all of your senses

Ad for Miami Tourisn served to a bot 🤖 with no pre-existing user IDs by Amobee DSP and Triplelift SSP. The source code of the Miami Tourism ad includes code from IAS.

5 people found dead in home near North 21st and West Wright streets in Milwaukee; police investigating deaths as homicides

Hannah Kirby and Drake Bentley Milwaukee Journal Sentinel

Ad for Bank of America Merrill Lynch - transacted by Omnicom - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Sharethrough SSP. Both vendors claim to partner with HUMAN Security.

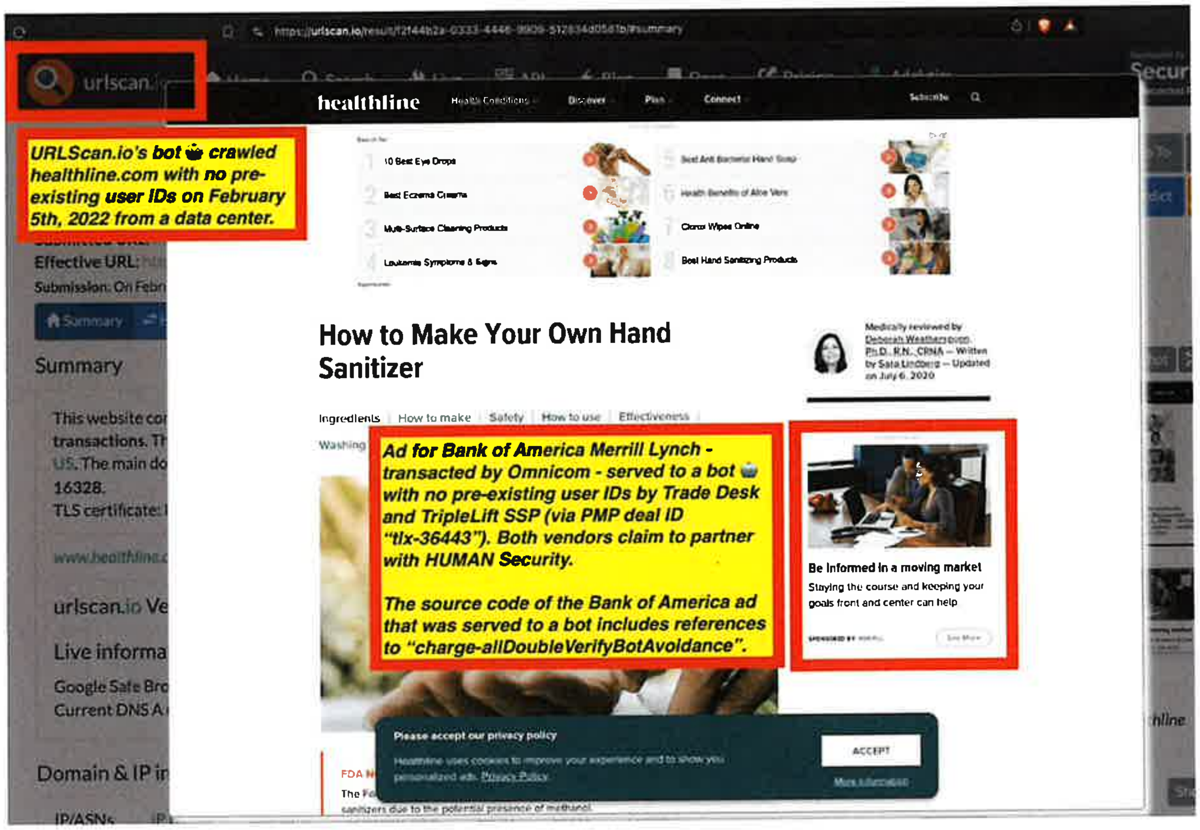
The source code of the Bank of America ad that was served to a bot includes references to "charge-allDoubleVerifyBotAvoidance".

Publisher has configured IAS publisher optimization tool on its page.

HTTP response from "pixel.adsafeprotected.com/services/pub" indicates that IAS labeled the bot 🤖 as valid, human traffic ("fr=false").

Screenshot of a Bank of America Merrill Lynch ad served to URLScan.io's bot and transacted by Omnicom, Trade Desk, and Sharethrough The source code of the Bank of America ad includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/1fe20077-1bab-415e-9f37-dbbd317563e9/

As another example, a Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling healthline.com on February 5th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Triplelift (via PMP deal ID "tlx-36443"), all three of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".



URLScan.io's bot 🤖 crawled healthline.com with no pre-existing user IDs on February 5th, 2022 from a data center.

Ad for Bank of America Merrill Lynch - transacted by Omnicom - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and TripleLift SSP (via PMP deal ID "tlx-36443"). Both vendors claim to partner with HUMAN Security.

The source code of the Bank of America ad that was served to a bot includes references to "charge-allDoubleVerifyBotAvoidance".

How to Make Your Own Hand Sanitizer

Medically reviewed by Deborah Weatherspoon, Ph.D., R.N., CRNA — Written by Sara Lindberg — Updated on July 6, 2020

Be Informed in a moving market

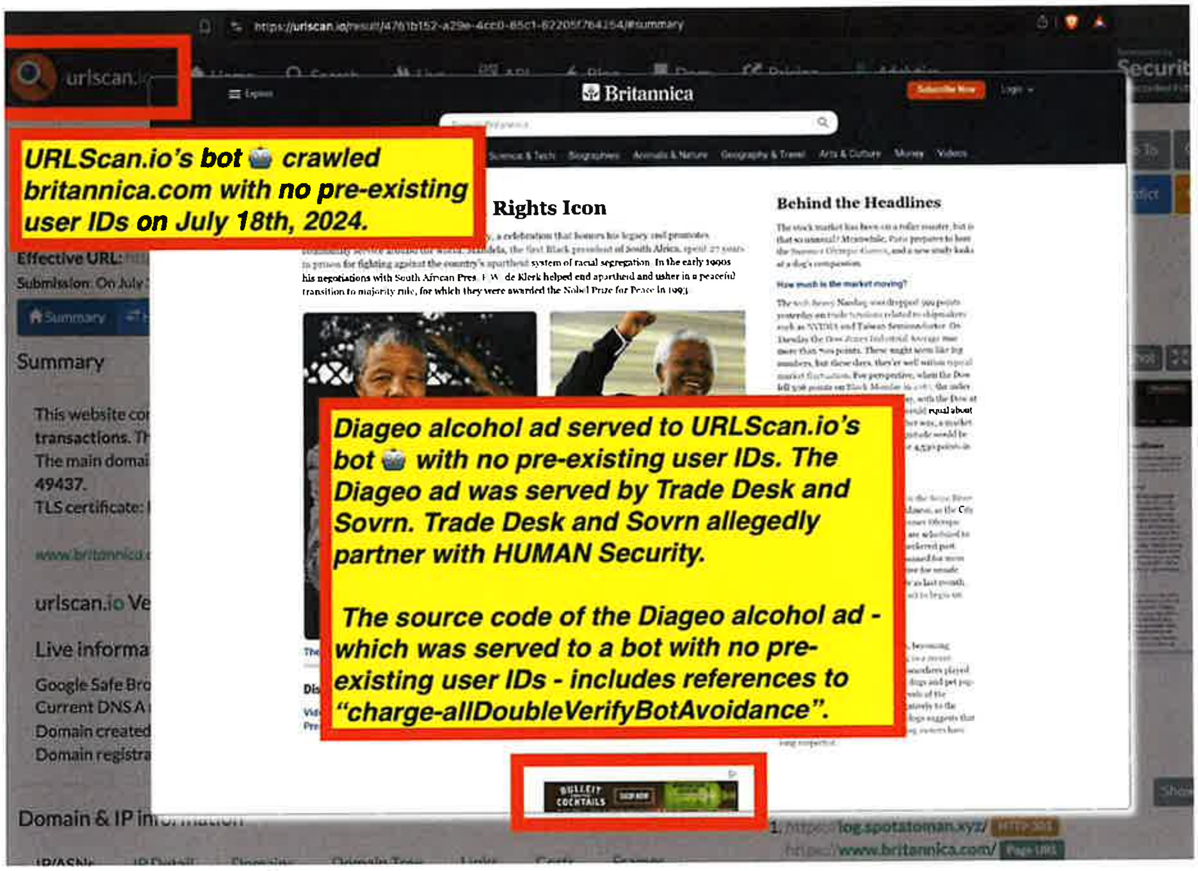
Staying the course and keeping your goals front and center can help

Please accept our privacy policy

Bank of America Merrill Lynch ad was served to URLScan.io's bot whilst the bot was crawling healthline.com on February 5th, 2022 from a data center. The Bank of America ad appears to have been transacted by Omnicom media agency and was served by Trade Desk and Triplelift, both of whom claim to partner with HUMAN Security, The Bank of America ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".

Source: https://urlscan.io/result/f2f44b2a-0333-4446-9909-512834d0581b/

As another example, a Diageo alcohol ad was served to URLScan.io's bot whilst the bot was crawling britannica.com on July 18th, 2024. The Diageo ad appears to have been served by Trade Desk and Sovrn, both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance".



URLScan.io's bot 🤖 crawled britannica.com with no pre-existing user IDs on July 18th, 2024.

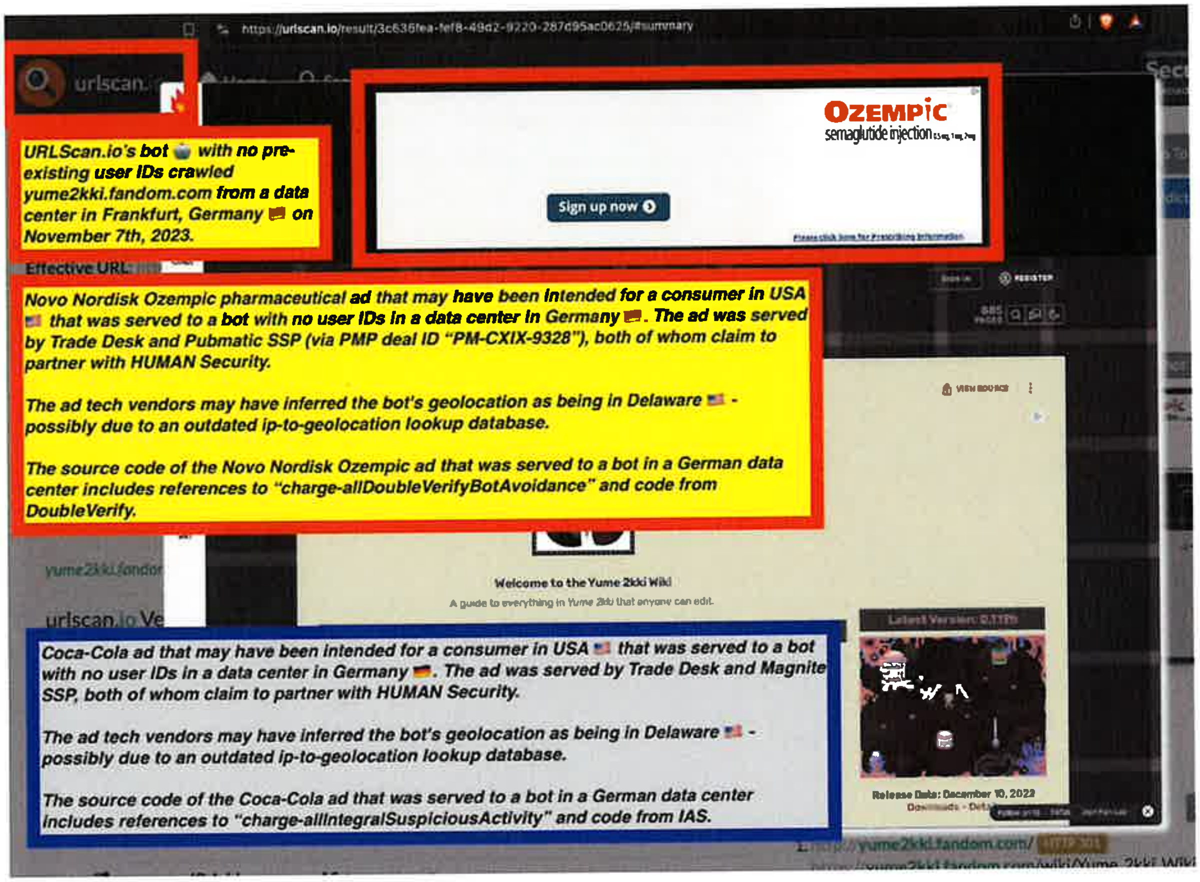
Diageo alcohol ad served to URLScan.io's bot 🤖 with no pre-existing user IDs. The Diageo ad was served by Trade Desk and Sovrn. Trade Desk and Sovrn allegedly partner with HUMAN Security.

The source code of the Diageo alcohol ad - which was served to a bot with no pre-existing user IDs - includes references to "charge-allDoubleVerifyBotAvoidance".

Diageo alcohol ad was served to URLScan.io's bot whilst the bot was crawling britannica.com on July 18th, 2024. The Diageo ad appears to have been served by Trade Desk and Sovrn, both of whom claim to partner with HUMAN Security, The Diageo alcohol ad includes references to DoubleVerify and "charge-allDoubleVerifyBotAvoidance". Source: https://urlscan.io/result/4761b152-a29e-4cc0-85c1-62205f764254/

As another example, an Novo Nordisk Ozempic ad was served to URLScan.io's bot whilst the bot was crawling yume2kki.fandom.com on November 7th, 2023 with no pre-existing user identifiers.

The Novo Nordisk Ozempic ad was served to a bot by Trade Desk and Pubmatic (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security. The source code of the Novo Nordisk ad includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. The ad appears to have been intended for a consumer in Delaware, USA but was served to a bot in a data center in Germany.



https://urlscan.io/result/3c636fea-fef8-49d2-9220-287d95ac0625/#summary

URLScan.io's bot 🤖 with no pre-existing user IDs crawled yume2kki.fandom.com from a data center in Frankfurt, Germany 🇩🇪 on November 7th, 2023.

Novo Nordisk Ozempic pharmaceutical ad that may have been intended for a consumer in USA 🇺🇸 that was served to a bot with no user IDs in a data center in Germany 🇩🇪. The ad was served by Trade Desk and Pubmatic SSP (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Delaware 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

The source code of the Novo Nordisk Ozempic ad that was served to a bot in a German data center includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

Coca-Cola ad that may have been intended for a consumer in USA 🇺🇸 that was served to a bot with no user IDs in a data center in Germany 🇩🇪. The ad was served by Trade Desk and Magnite SSP, both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Delaware 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

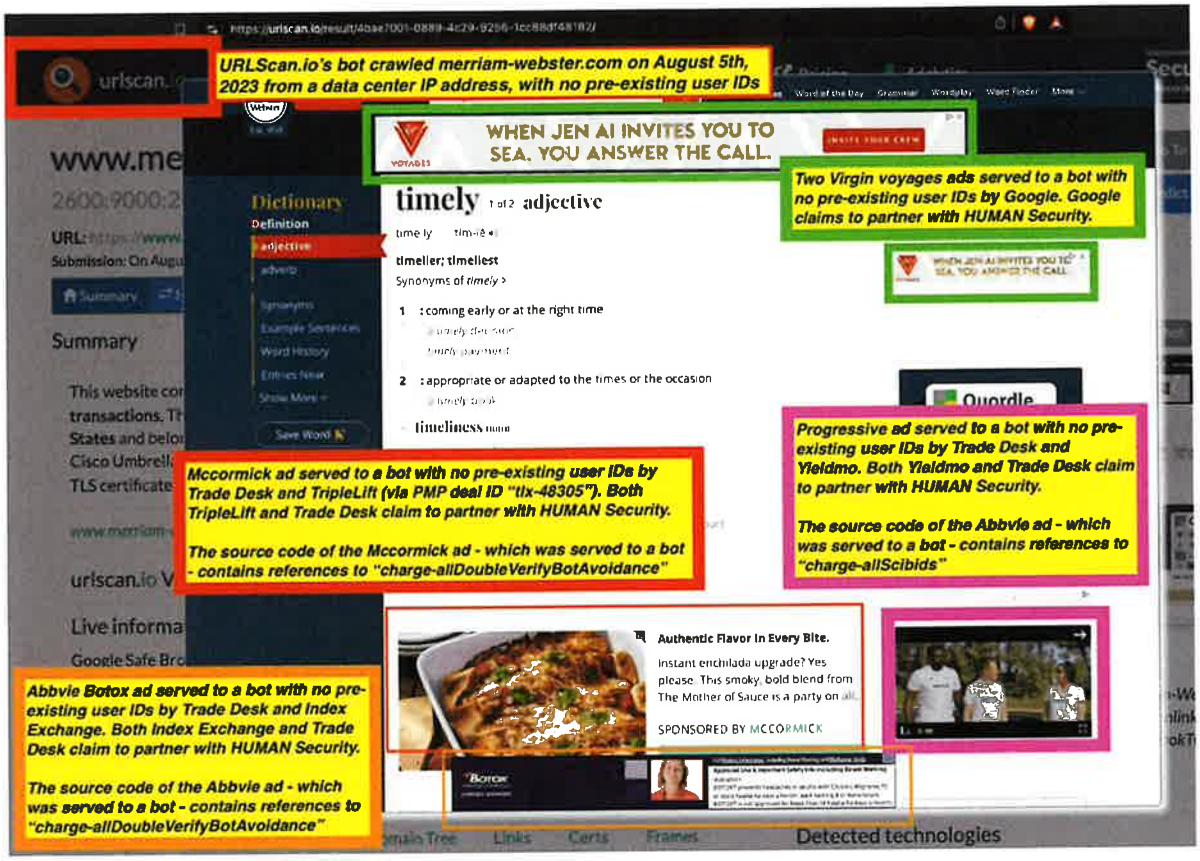
The source code of the Coca-Cola ad that was served to a bot in a German data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

urlscan.
OZEMPIC
semaglutide injection
Sign up now
Effective URL
yume2kki.fandom
urlscan.io Ve
Welcome to the Yume 2kki Wiki
A guide to everything in Yume 2kki that anyone can edit.
Latest Version: 0.117f
Release Date: December 10, 2022
https://yume2kki.fandom.com/

URLScan.io's bot 🤖 with no pre-existing user IDs crawled yume2kki.fandom.com from a data center in Frankfurt, Germany DE on November 7th, 2023. Novo Nordisk Ozempic pharmaceutical ad that may have been intended for a consumer in USA US that was served to a bot with no user IDs in a data center in Germany DE. The ad was served by Trade Desk and Pubmatic SSP (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Delaware US - possibly due to an outdated ip-to-geolocation lookup database. The source code of the Novo Nordisk Ozempic ad that was served to a bot in a German data center includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. Coca-Cola ad that may have been intended for a consumer in USA US that was served to a bot with no user IDs in a data center in Germany DE. The ad *was served by Trade Desk and Magnite SSP, both of whom claim to partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Delaware us - possibly due to an outdated ip-to-geolocation lookup database. The source code of the Coca-Cola ad that was served to a bot in a German data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.*

Source: https://urlscan.io/result/3c636fea-fef8-49d2-9220-287d95ac0625/

As another example, in the screenshot below one can observe ads for the following companies: Abbvie, Progressive insurance and Mccormick that were served to URLScan.io's bot on August 5th, 2023 whilst crawling merriam-webster.com. The Abbvie Botox ad appears to have been transacted by Trade Desk and Index Exchange, and its source code includes references to "charge-allDoubleVerifyBotAvoidance". The Mccormick ad appears to have been transacted by Trade Desk and Triplelift (via PMP deal ID "tlx-48305"), and its source code includes references to "charge-allDoubleVerifyBotAvoidance". The Progressive insurance ad appears to have been transacted by Trade Desk and Yieldmo, and its source code includes references to Scibids.



URLScan.io's bot crawled merriam-webster.com on August 5th, 2023 from a data center IP address, with no pre-existing user IDs

Two Virgin voyages ads served to a bot with no pre-existing user IDs by Google. Google claims to partner with HUMAN Security.

Mccormick ad served to a bot with no pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-48305"). Both TripleLift and Trade Desk claim to partner with HUMAN Security.

The source code of the Mccormick ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

Progressive ad served to a bot with no pre-existing user IDs by Trade Desk and Yieldmo. Both Yieldmo and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allScibids"

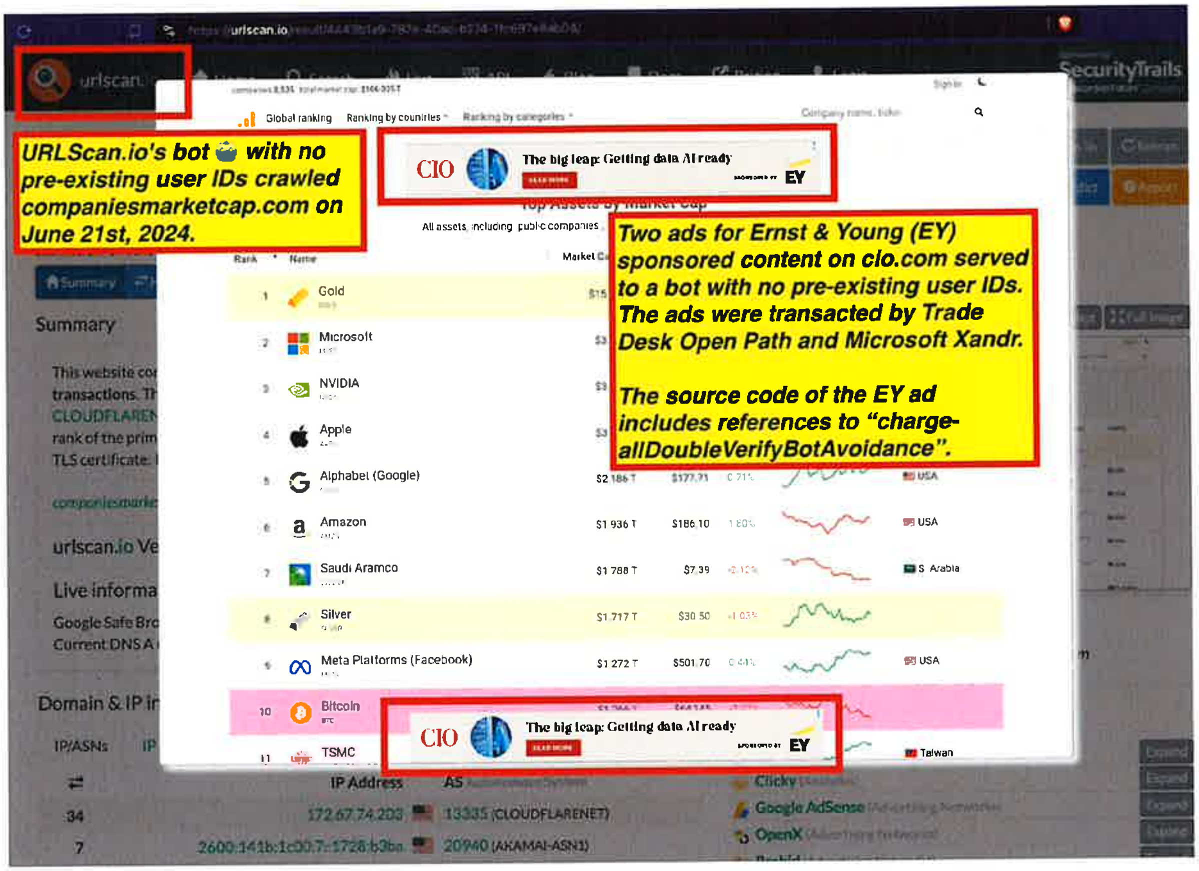
Abbvie Botox ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange. Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

Multiple DV360 and Trade Desk ads served to URLScan.io's bot, which was operating out of a data center with no pre-existing user IDs whilst crawling merriam-webster.com on August 5th, 2024. The bot was served two ads for Virgin Voyages by Google, and ads for Mccormick, Progressive, and Abbvie botox. The Mccormick and Abbvie ads' source code contains references to "charge-allDoubleVerifyBotAvoidance", whilst the Progressive video ad contains references to "charge-allScibids". The ads were transacted by Yieldmo, Index Exchange, and TripleLift, all of whom have many public statements about partnering with HUMAN Security. Source: https://urlscan.io/result/4bae7001-0889-4c29-9256-1cc88df48182/

As another example, in the screenshot below one can observe two ads for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on June 21st, 2024 whilst crawling companiesmarketcap.com. The EY ads appear to have been transacted by Trade Desk and Microsoft Xandr, both of whom partner with HUMAN

Security. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance."



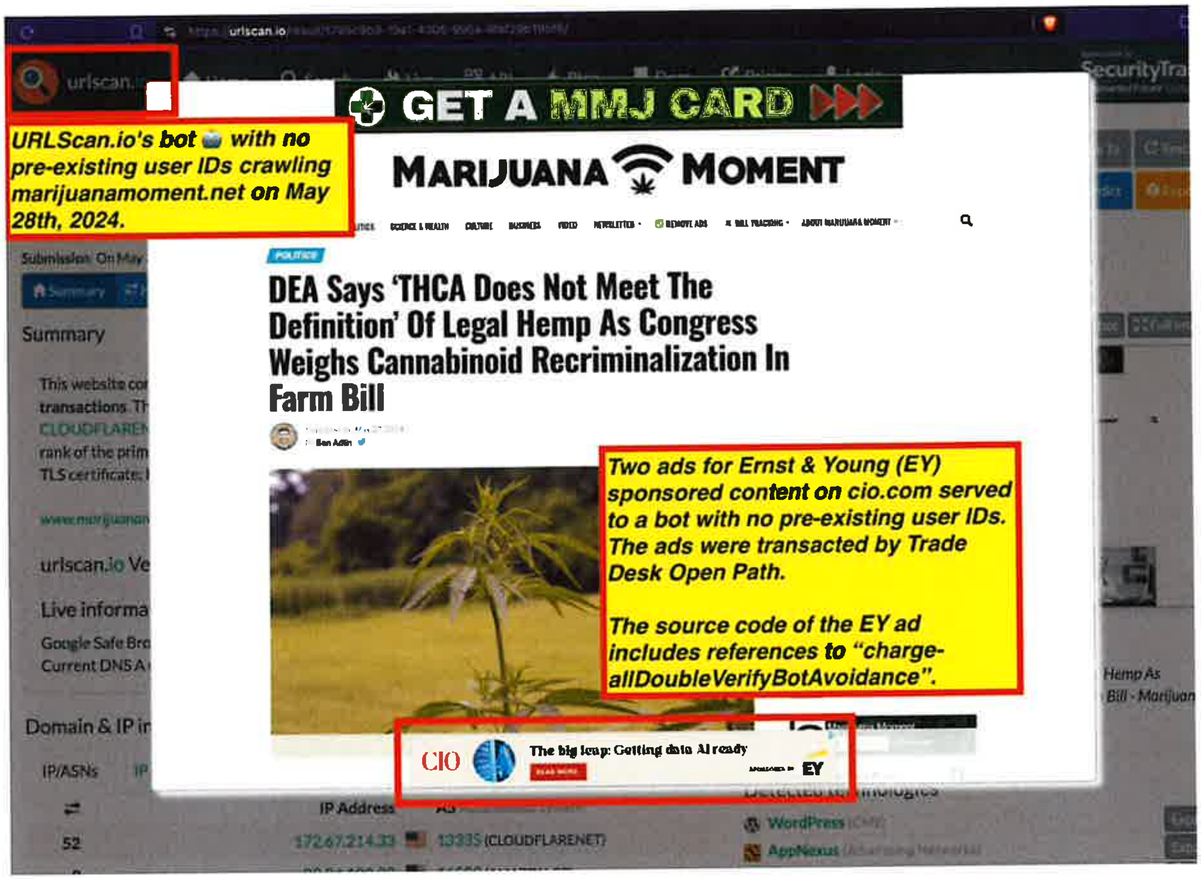
URLScan.io's bot 🤖 with no pre-existing user IDs crawled companiesmarketcap.com on June 21st, 2024.

Two ads for Ernst & Young (EY) sponsored content on cio.com served to a bot with no pre-existing user IDs. The ads were transacted by Trade Desk Open Path and Microsoft Xandr.

The source code of the EY ad includes references to "charge-allDoubleVerifyBotAvoidance".

Two ads for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on June 21st, 2024 whilst crawling companiesmarketcap.com. The EY ads appear to have been transacted by Trade Desk and Microsoft Xandr, both of whom partner with HUMAN Security. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/4443b1a9-787e-40ac-b274-1fc697e8ab04/#transactions

As another example, in the screenshot below one can see an ad for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on May 28th, 2024 whilst crawling marijuanamoment.net. The EY ads appear to have been transacted by Trade Desk Open Path. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance."



URLScan.io's **bot** 🤖 with **no** pre-existing user IDs crawling marijuanamoment.net **on** May 28th, 2024.

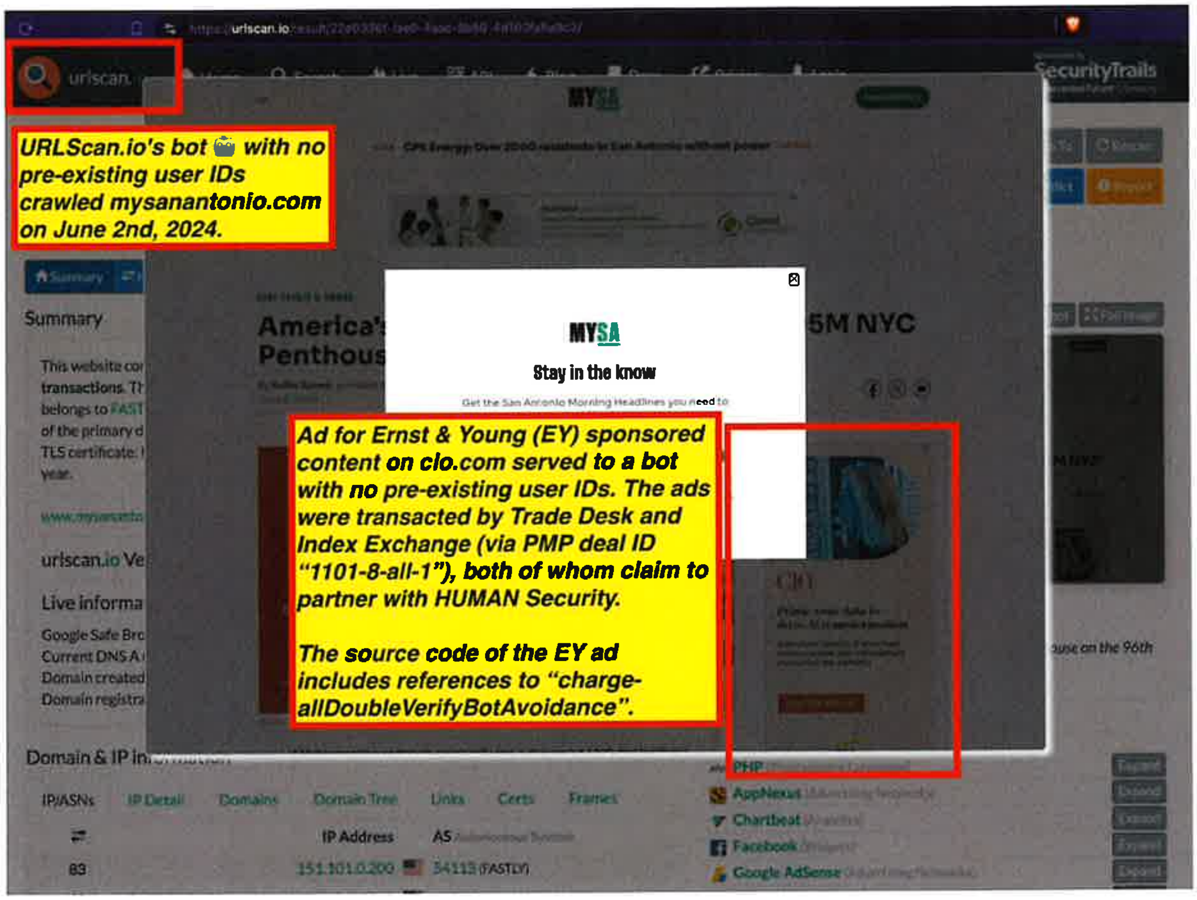
DEA Says 'THCA Does Not Meet The Definition' Of Legal Hemp As Congress Weighs Cannabinoid Recriminalization In Farm Bill

Two ads for Ernst & Young (EY) sponsored con**tent on** cio.com served to a bot with no pre-existing user IDs. The ads were transacted by Trade Desk Open Path.

The source code of the EY ad includes references **to** "charge-allDoubleVerifyBotAvoidance".

An ad for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on May 28th, 2024 whilst marijuanamoment.net on May 28th, 2024. The EY ads appear to have been transacted by Trade Desk Open Path. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/1795c9b3-19a1-4305-995a-6fef29b195f6/#summary

As another example, in the screenshot below one can see an ad for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on June 2nd, 2024 whilst the bot was crawling on marijuanamoment.net. The EY ads appear to have been transacted by Trade Desk and Index Exchange (via PMP deal ID "1101-8-all-1"), both of whom claim to partner with HUMAN Security. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance."



URLScan.io's bot 🤖 with no pre-existing user IDs crawled mysanantonio.com on June 2nd, 2024.

Ad for Ernst & Young (EY) sponsored content on cio.com served to a bot with no pre-existing user IDs. The ads were transacted by Trade Desk and Index Exchange (via PMP deal ID "1101-8-all-1"), both of whom claim to partner with HUMAN Security.

The source code of the EY ad includes references to "charge-allDoubleVerifyBotAvoidance".

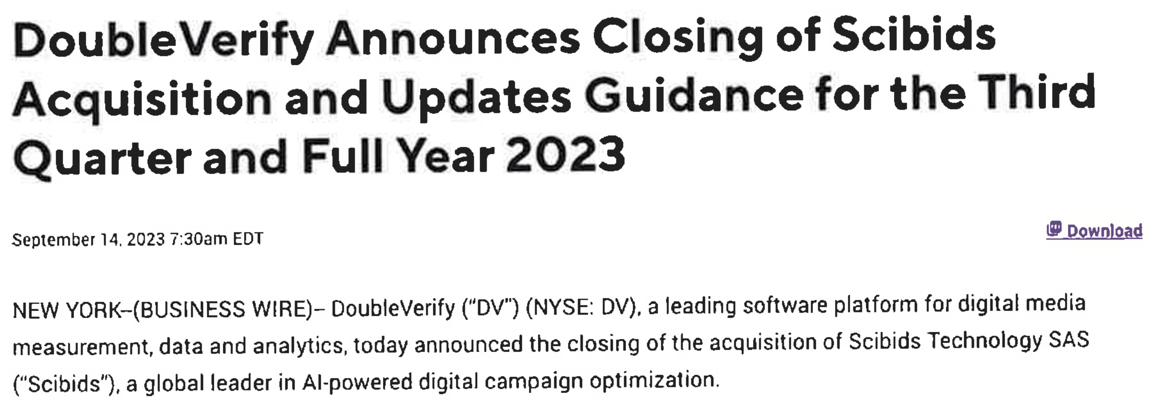
An ad for Ernst & Young (EY) sponsored content on cio.com served to URLScan.io's bot on June 2nd, 2024 whilst the bot was crawling mysanantonio.com. The source code of the EY ads includes references to "charge-allDoubleVerifyBotAvoidance." Source: https://urlscan.io/result/22e0336f-fae0-4aac-8b50-4d160fa5a9c2/#summary

Research Results: Brands whose ads appear to be mediated by DoubleVerify's Scibids AI technology and served to bots

In Q2 2023, DoubleVerify acquired a French company called Scibids. According to DoubleVerify, Scibids provides "AI-powered digital campaign optimization."

“Scibids pulls in impression-level data – including DoubleVerify attention data – to automate and optimize programmatic bids across demand-side platforms”, according to DoubleVerify CEO Mark Zagorski and reporting by AdExchanger. “It looks to minimize the bid to deliver the maximum return,” Zagorski said.

According to AdExchanger, “Scibids’ tech plugs directly into DSPs and gathers first- and third-party data as well as pricing, contextual, performance measurement, programmatic bidstream and measurement data, among others, from clients. Using this data, it dynamically creates “bespoke” bidding algorithms based on specific advertiser KPIs. Scibids is integrated with DSPs such as The Trade Desk, Google DV360, Microsoft’s Xandr and Comcast’s Beeswax. The algo does the trading, bid optimization and decision-making on its own, Zagorski said.”

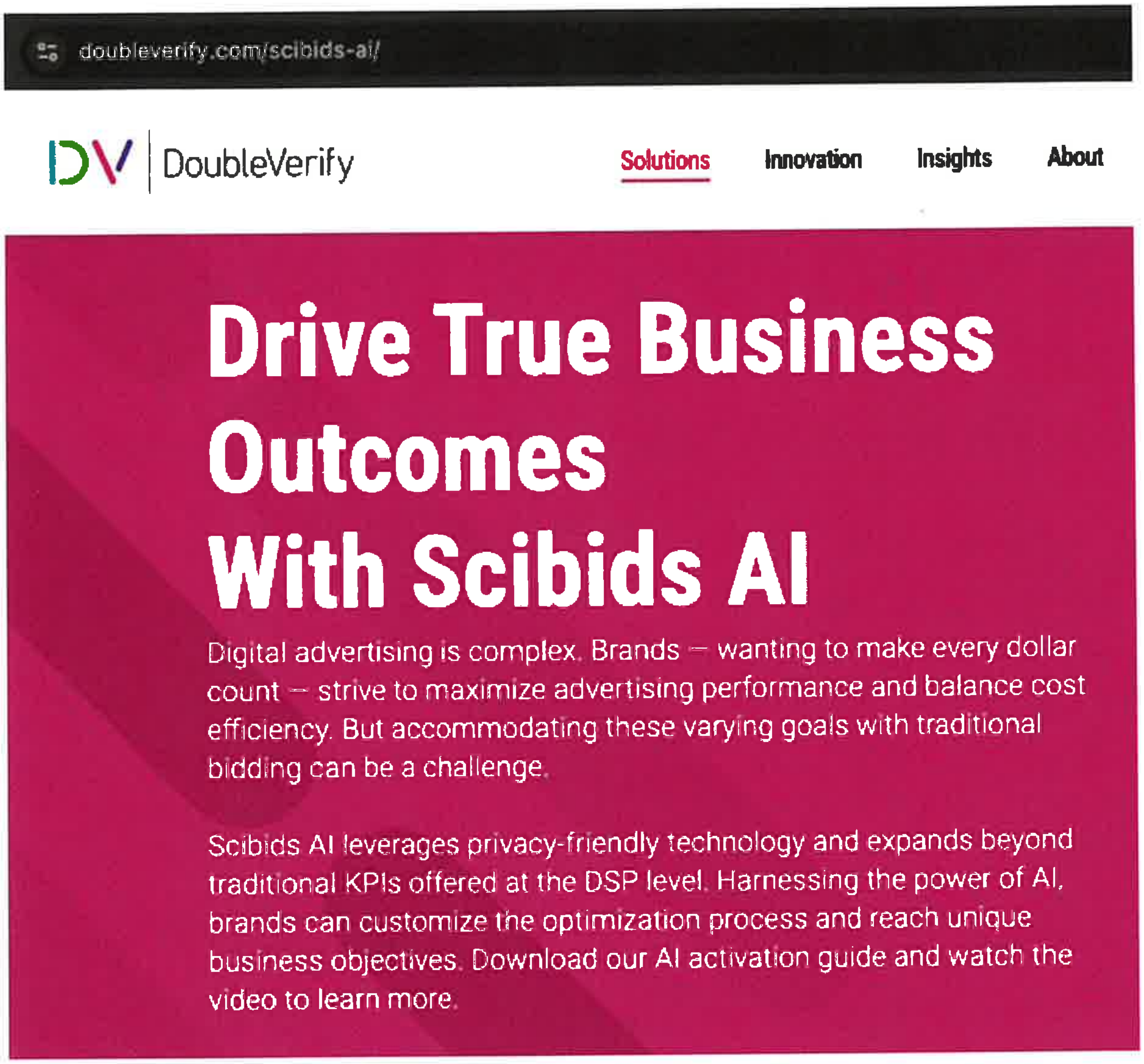


DoubleVerify Announces Closing of Scibids Acquisition and Updates Guidance for the Third Quarter and Full Year 2023

September 14, 2023 7:30am EDT

NEW YORK–(BUSINESS WIRE)– DoubleVerify (“DV”) (NYSE: DV), a leading software platform for digital media measurement, data and analytics, today announced the closing of the acquisition of Scibids Technology SAS (“Scibids”), a global leader in AI-powered digital campaign optimization.

Source: DoubleVerify



Drive True Business Outcomes With Scibids AI

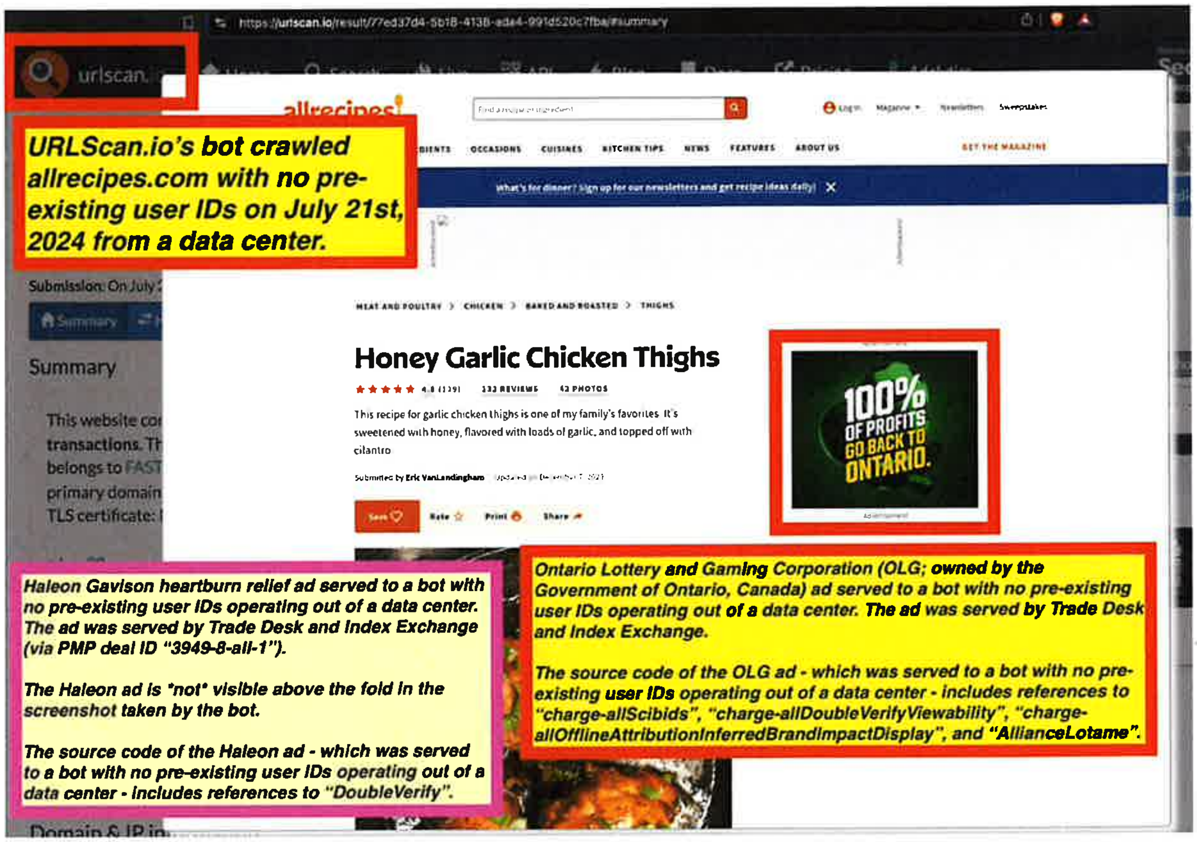
Digital advertising is complex. Brands – wanting to make every dollar count – strive to maximize advertising performance and balance cost efficiency. But accommodating these varying goals with traditional bidding can be a challenge.

Scibids AI leverages privacy-friendly technology and expands beyond traditional KPIs offered at the DSP level. Harnessing the power of AI, brands can customize the optimization process and reach unique business objectives. Download our AI activation guide and watch the video to learn more.

Source: DoubleVerify

The source code of several brands' ads - whose ads were served to declared bots operating out of known data center IP addresses or to URLScan.io bots - contained references to "charge-allScibids".

For example, in the screenshot below one can see an instance where URLScan.io's bot crawled the website allrecipes.com with no pre-existing user identifiers on July 21st, 2024 from a data center. The URLScan.io bot was shown an Ontario Lottery and Gaming Corporation (OLG; owned by the Government of Ontario, Canada) ad. The source code of the OLG ad includes references to "charge-allScibids", "charge-allDoubleVerifyViewability", "charge-allOfflineAttributionInferredBrandImpactDisplay", and "AllianceLotame".


https://urlscan.io/result/77ed37d4-5b18-4138-ada4-991d520c7fba/#summary
urlscan.io
allrecipes
What's for dinner? Sign up for our newsletters and get recipe ideas daily!
MEAT AND POULTRY > CHICKEN > BAKED AND ROASTED > THIGHS
Honey Garlic Chicken Thighs
132 REVIEWS
42 PHOTOS
This recipe for garlic chicken thighs is one of my family's favorites. It's sweetened with honey, flavored with loads of garlic, and topped off with cilantro
Submitted by Eric VanLandingham
Save
Rate
Print
Share
100% OF PROFITS GO BACK TO ONTARIO.
Summary
This website co transactions. Th belongs to FAST primary domain TLS certificate:
Domain & IP in

URLScan.io's bot crawled allrecipes.com with no pre-existing user IDs on July 21st, 2024 from a data center.

Haleon Gavison heartburn relief ad served to a bot with no pre-existing user IDs operating out of a data center. The ad was served by Trade Desk and Index Exchange (via PMP deal ID "3949-8-all-1").

The Haleon ad is *not* visible above the fold in the screenshot taken by the bot.

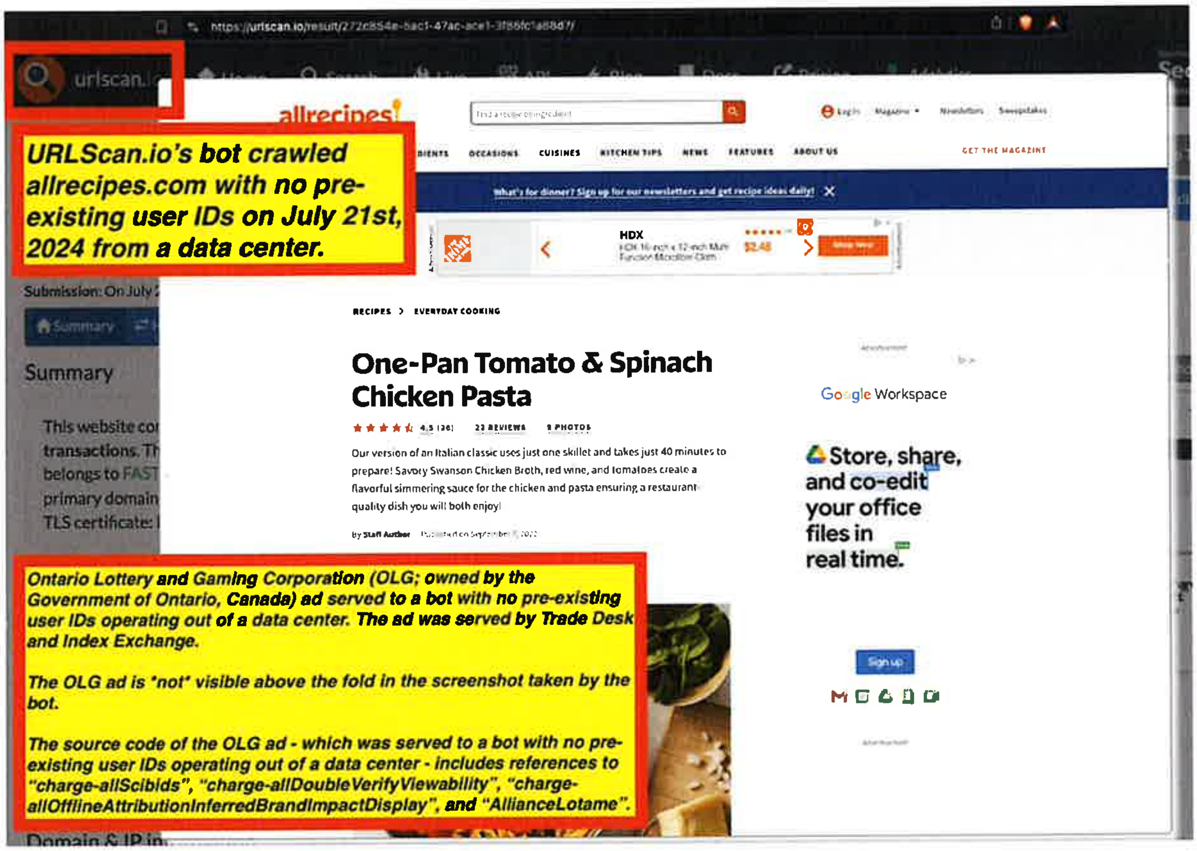
The source code of the Haleon ad - which was served to a bot with no pre-existing user IDs operating out of a data center - includes references to "DoubleVerify".

Ontario Lottery and Gaming Corporation (OLG; owned by the Government of Ontario, Canada) ad served to a bot with no pre-existing user IDs operating out of a data center. The ad was served by Trade Desk and Index Exchange.

The source code of the OLG ad - which was served to a bot with no pre-existing user IDs operating out of a data center - includes references to "charge-allScibids", "charge-allDoubleVerifyViewability", "charge-allOfflineAttributionInferredBrandImpactDisplay", and "AllianceLotame".

Screenshot of an Ontario Lottery and Gaming Corporation (OLG; owned by the Government of Ontario, Canada) ad shown to URLScan.io's bot. The source code of the OLG ad includes references to "charge-allScibids", "charge-allDoubleVerifyViewability", "charge-allOfflineAttributionInferredBrandImpactDisplay", and "AllianceLotame". Not visible in the screenshot is an ad from Haleon for Gavison heartburn relief. The Haleon Gavison ad was transacted by Trade Desk and Index Exchange (via PMP deal ID "3949-8-all-1") and includes references to "DoubleVerify". Source: https://urlscan.io/result/77ed37d4-5b18-4138-ada4-991d520c7fba/

As another example, in the screenshot below one can see an instance where URLScan.io's bot crawled the website allrecipes.com with no pre-existing user identifiers on July 21st, 2024 from a data center. The URLScan.io bot was shown an Ontario Lottery and Gaming Corporation (OLG; owned by the Government of Ontario, Canada) ad, which is not viewable in the screenshot. The source code of the OLG ad includes references to “charge-allScibids”, “charge-allDoubleVerifyViewability”, “charge-allOfflineAttributionInferredBrandImpactDisplay”, and “AllianceLotame”. The URLScan.io bot was also shown an ad for Google Workspace by Google.



URLScan.io’s bot crawled allrecipes.com with no pre-existing user IDs on July 21st, 2024 from a data center.

RECIPES > EVERYDAY COOKING

One-Pan Tomato & Spinach Chicken Pasta

Our version of an Italian classic uses just one skillet and takes just 40 minutes to prepare! Savory Swanson Chicken Broth, red wine, and tomatoes create a flavorful simmering sauce for the chicken and pasta ensuring a restaurant quality dish you will both enjoy!

Ontario Lottery and Gaming Corporation (OLG; owned by the Government of Ontario, Canada) ad served to a bot with no pre-existing user IDs operating out of a data center. The ad was served by Trade Desk and Index Exchange.

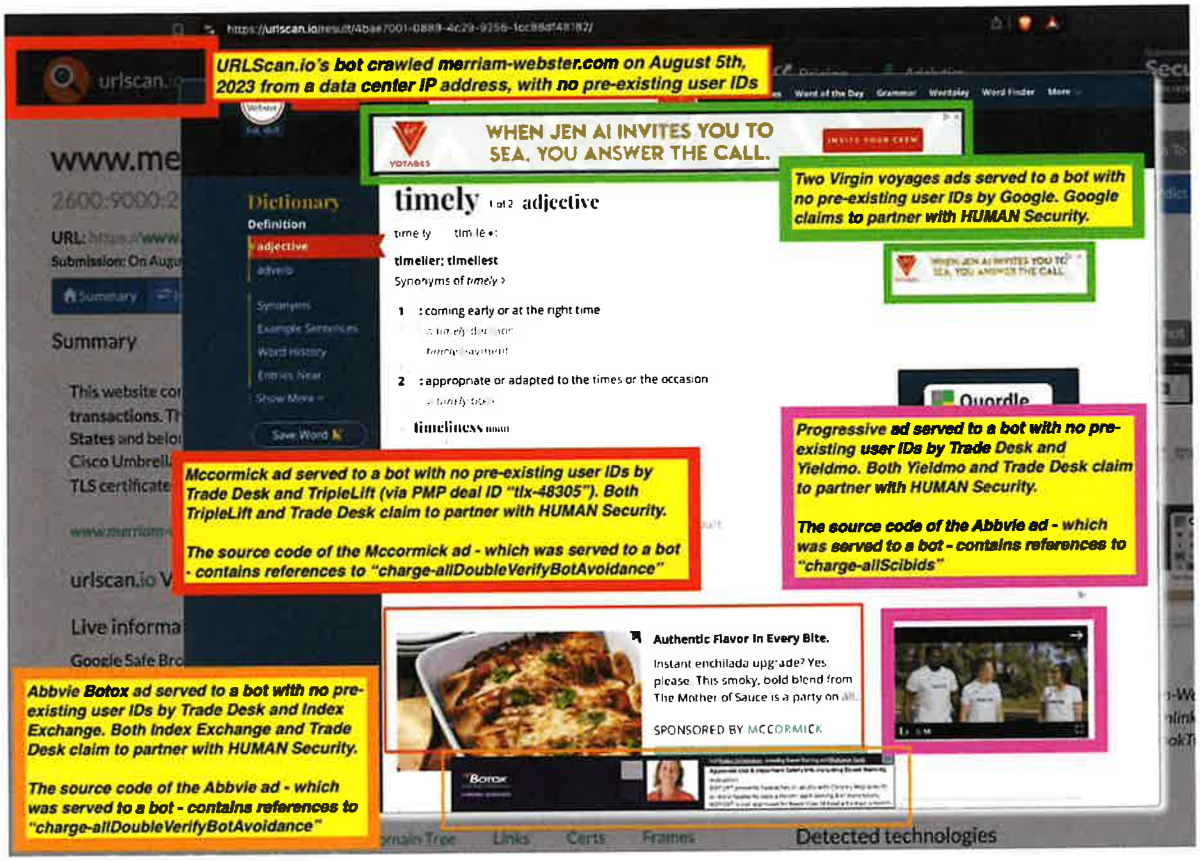
The OLG ad is *not* visible above the fold in the screenshot taken by the bot.

The source code of the OLG ad - which was served to a bot with no pre-existing user IDs operating out of a data center - includes references to “charge-allScibids”, “charge-allDoubleVerifyViewability”, “charge-allOfflineAttributionInferredBrandImpactDisplay”, and “AllianceLotame”.

https://urlscan.io/result/272c854e-5ac1-47ac-ace1-3f86fc1a88d7/
urlscan.io
allrecipes
Summary
HDX
$2.48
4.5 (36)
22 REVIEWS
9 PHOTOS
By Staff Author
Google Workspace
Store, share, and co-edit your office files in real time.
Sign up

Screenshot of URLScan.io’s bot crawling allrecipes.com on July 21st, 2024, whilst being shown an OLG ad that contains references to “charge-allScibids”. Source: https://urlscan.io/result/272c854e-5ac1-47ac-ace1-3f86fc1a88d7/

As another example, in the screenshot below one can see a Progressive insurance ad that was served to URLScan.io’s bot whilst the bot was crawling the website merriam-webster.com with no pre-existing user identifiers on August 5th, 2023 from a data center. The source code of the Progressive insurance ad includes references to “charge-allScibids”.


https://urlscan.io/result/4bae7001-0889-4c29-9256-1cc88df48182/
urlscan.io
www.me
Dictionary
Definition
adjective
timely
WHEN JEN AI INVITES YOU TO SEA. YOU ANSWER THE CALL.
Quordle
Authentic Flavor In Every Bite.
Instant enchilada upgrade? Yes please. This smoky, bold blend from The Mother of Sauce is a party on all.
SPONSORED BY MCCORMICK
Botox
Detected technologies

URLScan.io's bot crawled merriam-webster.com on August 5th, 2023 from a data center IP address, with no pre-existing user IDs

Two Virgin voyages ads served to a bot with no pre-existing user IDs by Google. Google claims to partner with HUMAN Security.

Progressive ad served to a bot with no pre-existing user IDs by Trade Desk and Yieldmo. Both Yieldmo and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allScibids"

Mccormick ad served to a bot with no pre-existing user IDs by Trade Desk and TripleLift (via PMP deal ID "tlx-48305"). Both TripleLift and Trade Desk claim to partner with HUMAN Security.

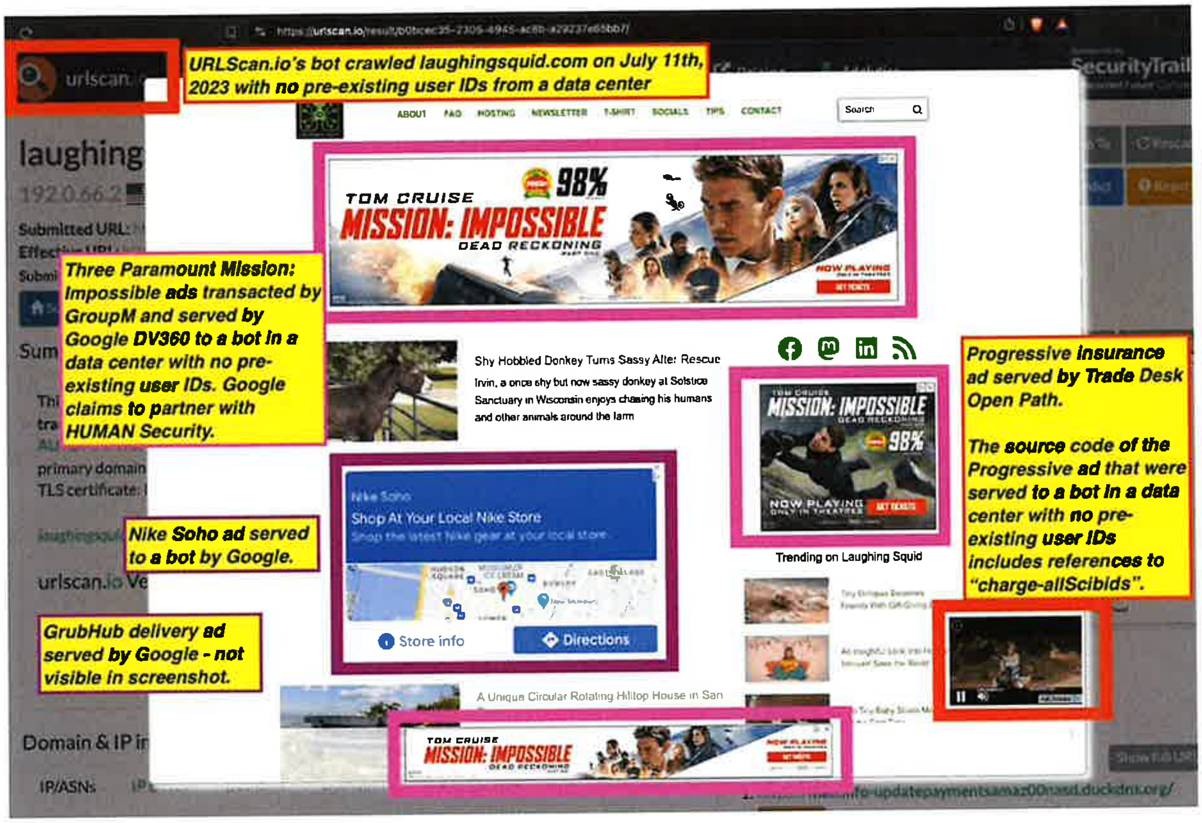
The source code of the Mccormick ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

Abbvie Botox ad served to a bot with no pre-existing user IDs by Trade Desk and Index Exchange. Both Index Exchange and Trade Desk claim to partner with HUMAN Security.

The source code of the Abbvie ad - which was served to a bot - contains references to "charge-allDoubleVerifyBotAvoidance"

Multiple DV360 and Trade Desk ads served to URLScan.io's bot, which was operating out of a data center with no pre-existing user IDs whilst crawling merriam-webster.com on August 5th, 2024. The bot was served two ads for Virgin Voyages by Google, and ads for Mccormick, Progressive, and Abbvie botox. The Mccormick and Abbvie ads' source code contains references to "charge-allDoubleVerifyBotAvoidance", whilst the Progressive video ad contains references to "charge-allScibids". The ads were transacted by Yieldmo, Index Exchange, and TripleLift, all of whom have many public statements about partnering with HUMAN Security. Source: https://urlscan.io/result/4bae7001-0889-4c29-9256-1cc88df48182/

As another example, in the screenshot below one can see a muted, auto-playing, out-stream video Progressive insurance ad that was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website laugingsquid.com on July 11th, 2023 from a data center. The source code of the Progressive insurance ad includes references to "charge-allScibids".



URLScan.io's bot crawled laughingsquid.com on July 11th, 2023 with **no** pre-existing user IDs from a data center

Three Paramount Mission: Impossible ads transacted by GroupM and served by Google DV360 to a bot in a data center with no pre-existing user IDs. Google claims to partner with HUMAN Security.

Shy Hobbled Donkey Turns Sassy After Rescue

Irvin, a once shy but now sassy donkey at Solstice Sanctuary in Wisconsin enjoys chasing his humans and other animals around the farm

Nike Soho ad served to a bot by Google.

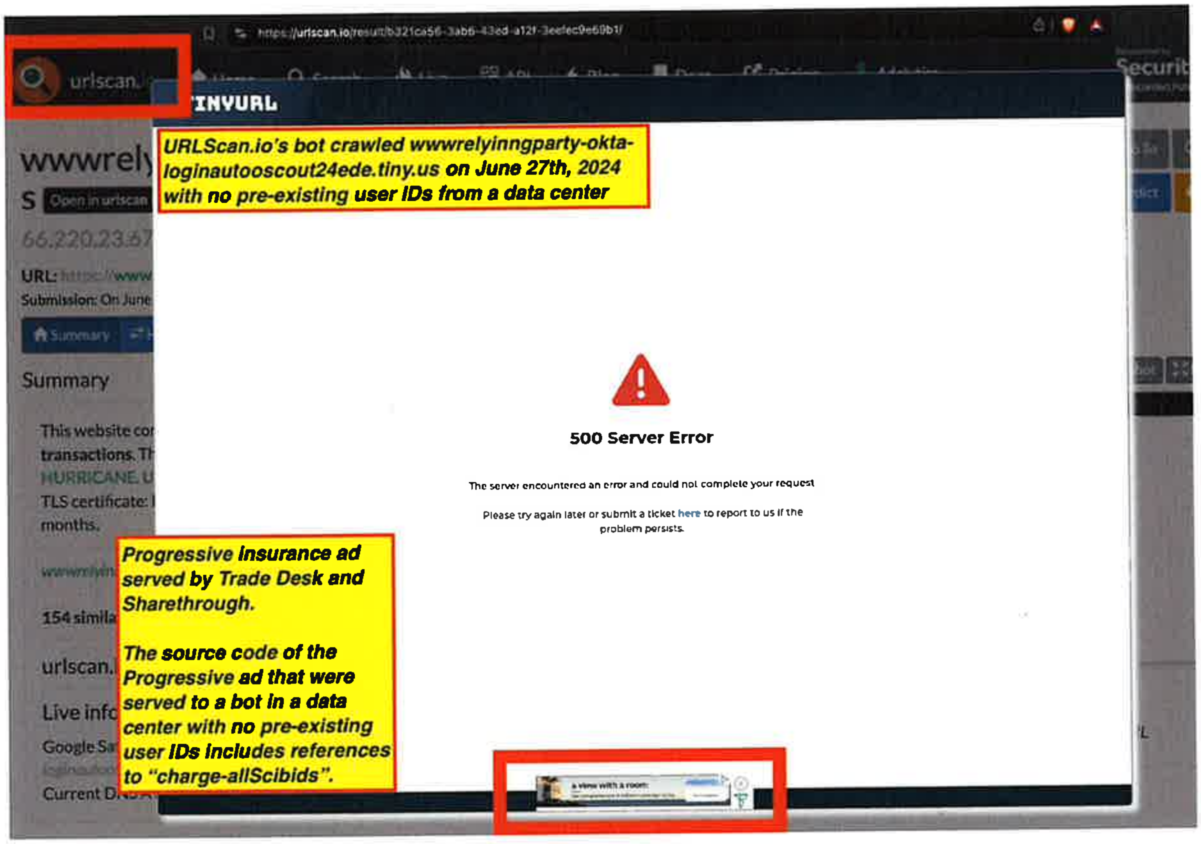
GrubHub delivery ad served by Google - not visible in screenshot.

Progressive insurance ad served by Trade Desk Open Path.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids".

Screenshot of URLScan.io's bot crawling laugingsquid.com on July 11th, 203, whilst being shown a Progressive insurance ad that contains references to "charge-allScibids". Source: https://urlscan.io/result/b0bcec35-2305-4945-ac8b-a29237e65bb7/#summary

As another example, in the screenshot below one can see a Progressive insurance ad that was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website wwwrelyinngparty-okta-loginautooscout24ede.tiny.us on June 27th, 2024 from a data center. The website generated a 500 HTTP status error, meaning the website did not load properly when the bot crawled the page. The source code of the Progressive insurance ad includes references to "charge-allScibids".



URLScan.io's bot crawled wwwrelyinngparty-okta-loginautooscout24ede.tiny.us on June 27th, 2024 with no pre-existing user IDs from a data center

500 Server Error

The server encountered an error and could not complete your request

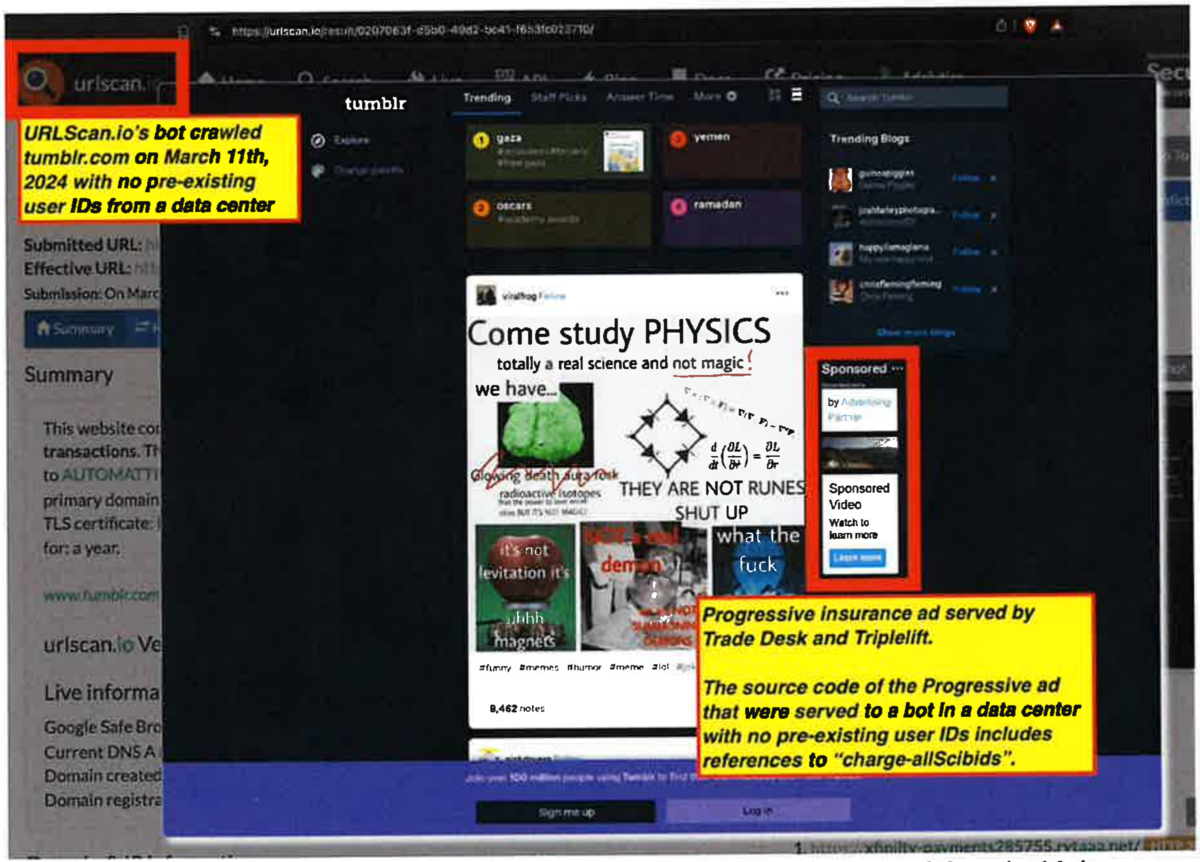
Please try again later or submit a ticket here to report to us if the problem persists.

Progressive insurance ad served by Trade Desk and Sharethrough.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids".

Screenshot of URLScan.io's bot crawling wwwrelyinngparty-okta-loginautooscout24ede.tiny.us on June 27th, 2024, whilst being shown a Progressive ad that contains references to "charge-allScibids". Source: https://urlscan.io/result/b321ca56-3ab6-43ed-a12f-3eefec9e69b1/

As another example, in the screenshot below one can see a Progressive insurance ad that was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website tumblr.com on March 11th, 2024 from a data center. The source code of the Progressive insurance ad includes references to "charge-allScibids".



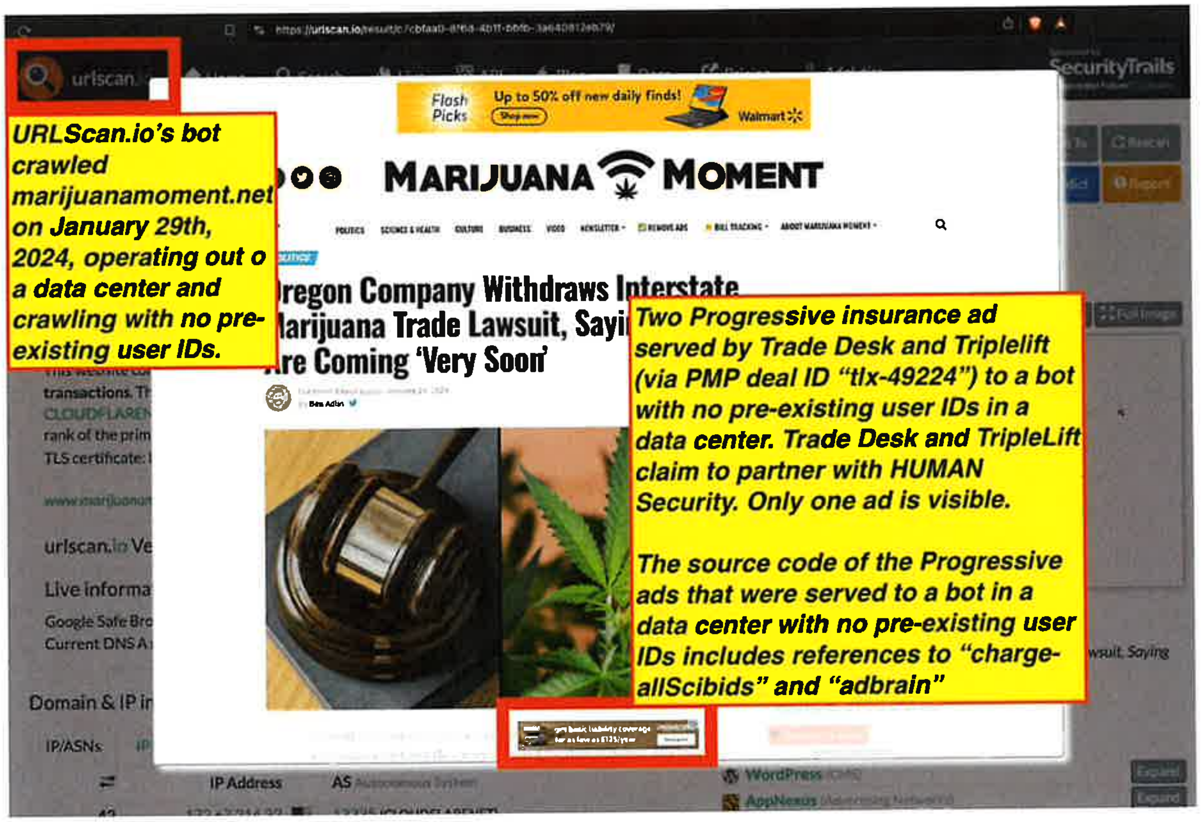
URLScan.io's bot crawled tumblr.com on March 11th, 2024 with no pre-existing user IDs from a data center

Progressive insurance ad served by Trade Desk and Triplelift.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids".

Screenshot of URLScan.io's bot crawling tumblr.com on March 11th, 2024, whilst being shown a Progressive ad that contains references to "charge-allScibids". Source: https://urlscan.io/result/0207063f-d5b0-49d2-bc41-f6b3fc023710/

As another example, in the screenshot below one can see a Progressive insurance ad that was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website marijuanamoment.net on January 29th, 2024 from a data center. The source code of the Progressive insurance ad includes references to "charge-allScibids".


urlscan
Flash Picks
Up to 50% off new daily finds!
Walmart
MARIJUANA MOMENT
SecurityTrails
regon Company Withdraws Interstate
larijuana Trade Lawsuit, Sayi
re Coming 'Very Soon'

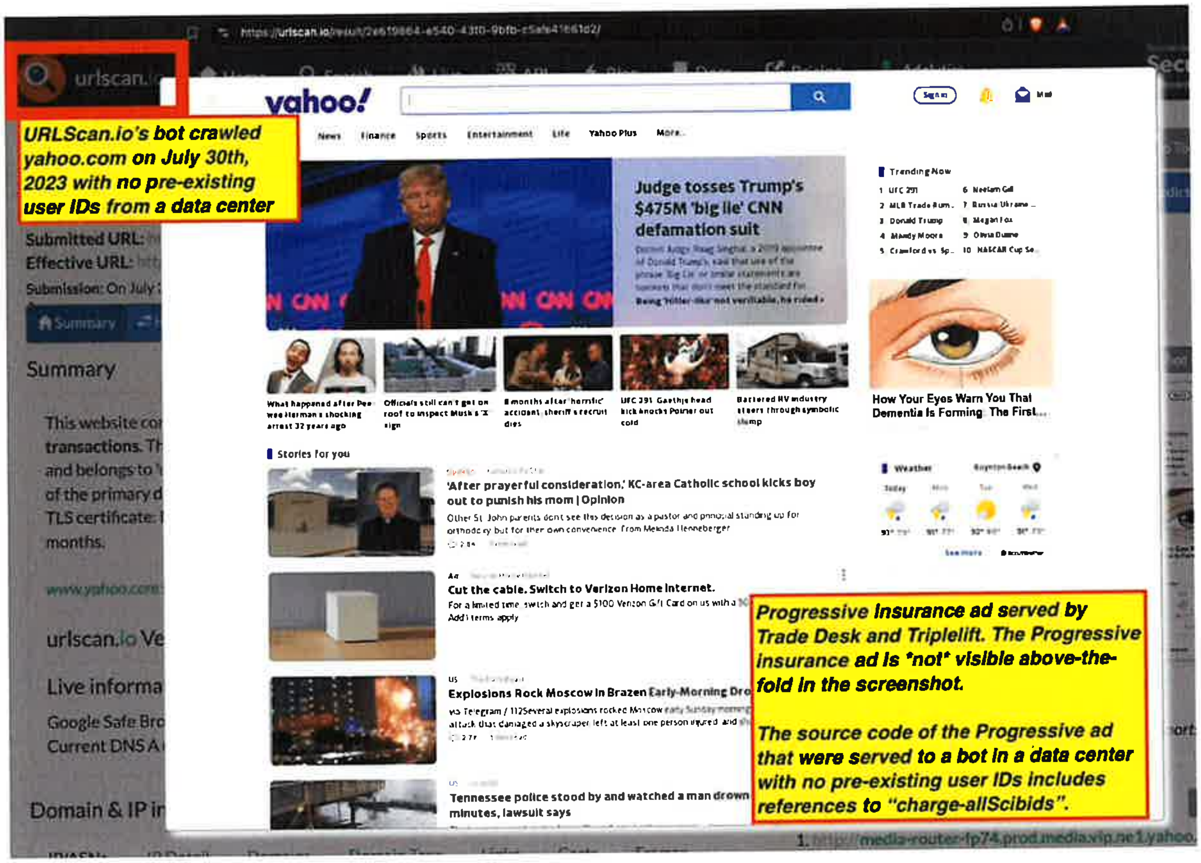
URLScan.io's bot crawled marijuanamoment.net on January 29th, 2024, operating out o a data center and crawling with no pre-existing user IDs.

Two Progressive insurance ad served by Trade Desk and Triplelift (via PMP deal ID "tlx-49224") to a bot with no pre-existing user IDs in a data center. Trade Desk and TripleLift claim to partner with HUMAN Security. Only one ad is visible.

The source code of the Progressive ads that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain"

Screenshot of URLScan.io's bot crawling marijunamoment.net.com on January 29th, 2024, whilst being shown a Progressive ad that contains references to "charge-allScibids". Source: https://urlscan.io/result/c7cbfaa0-8f6d-4b1f-bbfb-3a640812eb79/

As another example, a Progressive insurance ad was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website yahoo.com on July 30th, 2023 from a data center. The source code of the Progressive insurance ad includes references to "charge-allScibids". The Progress ad is not visible above-the-fold in the screenshot generated by URLScan.io's bot.


urlscan.io
yahoo!
News
Finance
Sports
Entertainment
Life
Yahoo Plus
More...
Judge tosses Trump's $475M 'big lie' CNN defamation suit
Trending Now
Stories for you
'After prayerful consideration,' KC-area Catholic school kicks boy out to punish his mom | Opinion
Cut the cable. Switch to Verizon Home Internet.
Explosions Rock Moscow In Brazen Early-Morning Dro
Tennessee police stood by and watched a man drown minutes, lawsuit says
How Your Eyes Warn You That Dementia Is Forming. The First...
Weather
Submitted URL:
Effective URL:
Summary
urlscan.io Ve
Live informa
Domain & IP ir

URLScan.io's bot crawled yahoo.com on July 30th, 2023 with no pre-existing user IDs from a data center

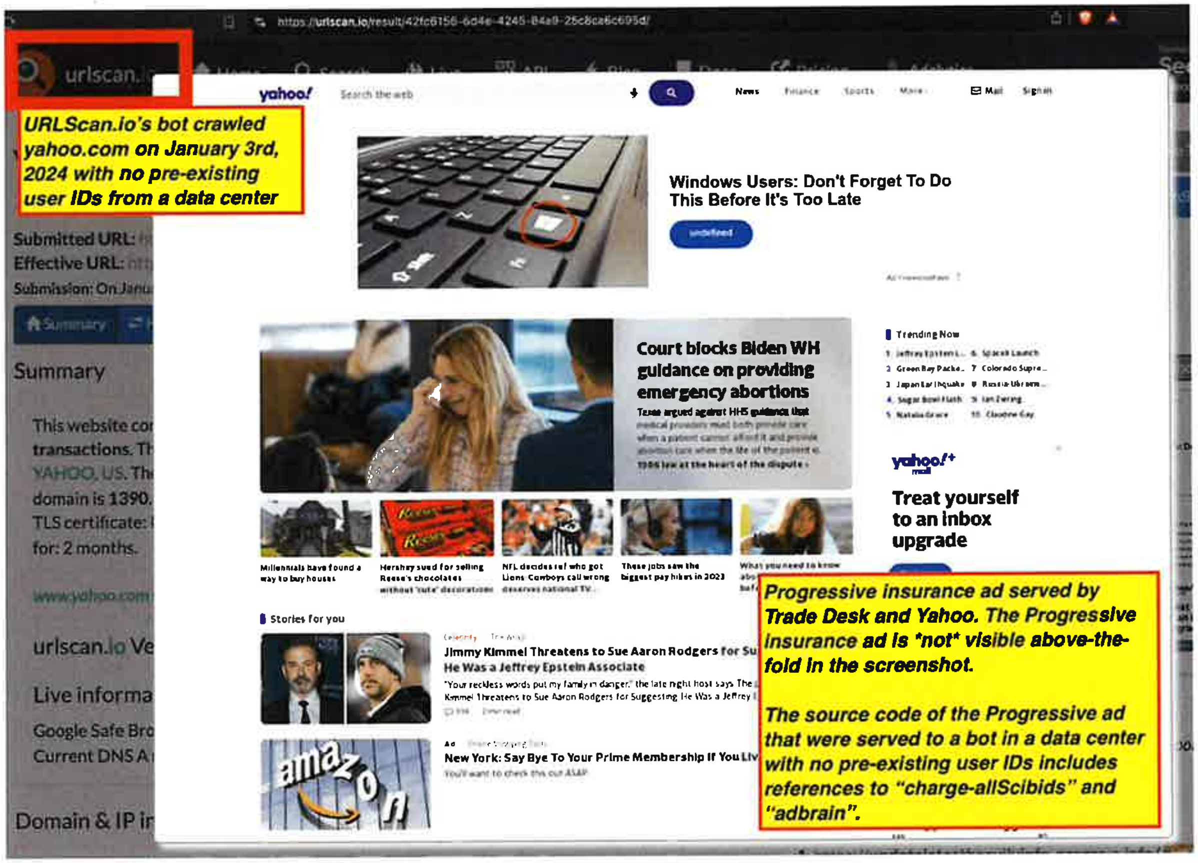
Progressive Insurance ad served by Trade Desk and Triplelift. The Progressive insurance ad is *not* visible above-the-fold in the screenshot.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids".

Screenshot of URLScan.io's bot crawling yahoo.com on July 30th, 2023 whilst being shown a Progressive ad that contains references to "charge-allScibids". The Progressive ad is not visible above-the-fold in the screenshot generated by the bot. Source: https://urlscan.io/result/2e619864-e540-43f0-9bfb-c5afe41661d2/

As another example, a Progressive insurance ad was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website yahoo.com on January 3rd, 2024 from a data center. The source code of the Progressive insurance ad includes references to "charge-allScibids". The Progress ad is not visible above-the-fold in the screenshot generated by URLScan.io's bot.

https://adalytics.io/blog/prebid-bot-filtration



URLScan.io's bot crawled yahoo.com on January 3rd, 2024 with no pre-existing user IDs from a data center

Submitted URL:
Effective URL:
Submission: On Janu

This website co
transactions. Th
YAHOO, US. Th
domain is 1390.
TLS certificate:
for: 2 months.

www.yahoo.com

urlscan.io Ve

Live informa

Google Safe Bro
Current DNS A

Domain & IP in

Windows Users: Don't Forget To Do This Before It's Too Late

Court blocks Biden WH guidance on providing emergency abortions

Texas argued against HHS guidance that medical providers must both provide care when a patient cannot afford it and provide abortion care when the life of the patient is … 1986 law at the heart of the dispute ›

Millennials have found a way to buy houses

Hershey sued for selling Reese's chocolates without 'cute' decorations

NFL decides ref who got Lions-Cowboys call wrong deserves national TV…

These jobs saw the biggest pay hikes in 2023

What you need to know

Treat yourself to an inbox upgrade

Jimmy Kimmel Threatens to Sue Aaron Rodgers for Su He Was a Jeffrey Epstein Associate

"Your reckless words put my family in danger," the late night host says. The Kimmel Threatens to Sue Aaron Rodgers for Suggesting He Was a Jeffrey

Ad

New York: Say Bye To Your Prime Membership If You Liv

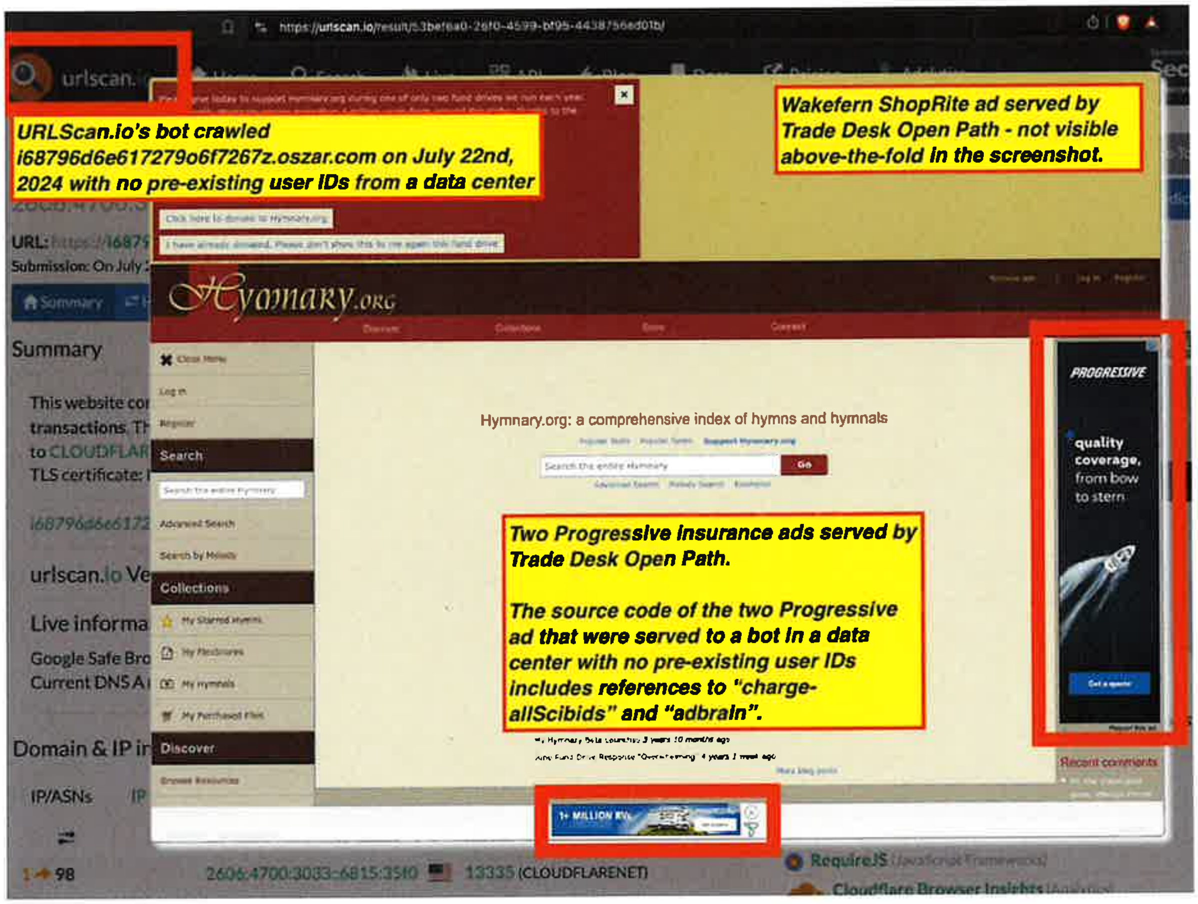
You'll want to check this out ASAP

Progressive insurance ad served by Trade Desk and Yahoo. The Progressive insurance ad is *not* visible above-the-fold in the screenshot.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain".

Screenshot of URLScan.io's bot crawling yahoo.com on January 3rd, 2024 whilst being shown a Progressive ad that contains references to "charge-allScibids". The Progressive ad is not visible above-the-fold in the screenshot generated by the bot. Source: https://urlscan.io/result/42fc6156-6d4e-4245-84a9-25c8ca6c695d/

As another example, two Progressive insurance ads were served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website i68796d6e617279o6f7267z.oszar.com on July 22nd, 2024 from a data center. The source code of the Progressive insurance ads includes references to "charge-allScibids" and "adbrain".



URLScan.io's bot crawled i68796d6e617279o6f7267z.oszar.com on July 22nd, 2024 with no pre-existing user IDs from a data center

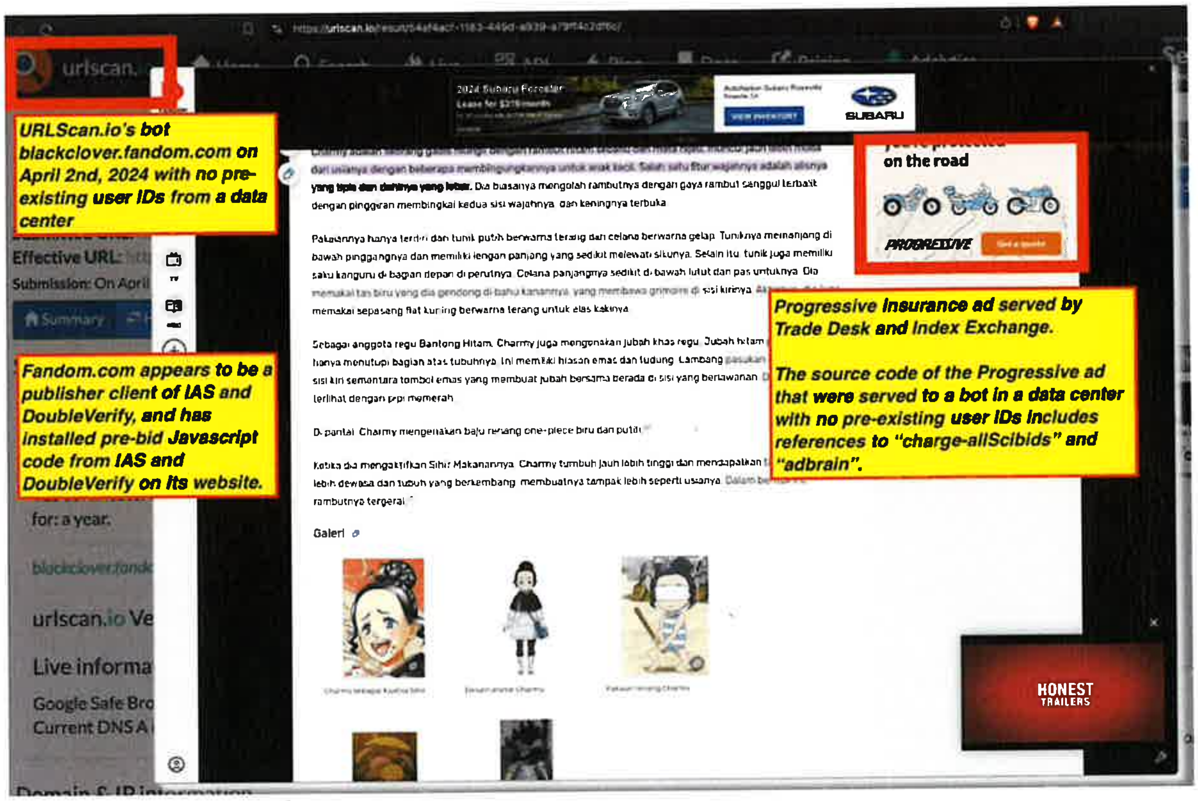
Wakefern ShopRite ad served by Trade Desk Open Path - not visible above-the-fold in the screenshot.

Two Progressive insurance ads served by Trade Desk Open Path.

The source code of the two Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain".

Screenshot of URLScan.io's bot crawling i68796d6e617279o6f7267z.oszar.com on July 22nd, 2024 whilst being shown two Progressive insurance ads that contain references to "charge-allScibids" and "adbrain". Source: https://urlscan.io/result/53bef6a0-26f0-4599-bf95-4438756ed01b/#summary

As another example, a Progressive insurance ad was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website blackclover.fandom.com on April 2nd, 2024 from a data center. The source code of the Progressive insurance ads includes references to "charge-allScibids" and "adbrain". The publisher fandom.com appears to employ both IAS and DoubleVerify's publisher optimization tools on its web pages. Fandom lists IAS and DoubleVerify as "partners" on its media kit for prospective advertisers.



URLScan.io's bot blackclover.fandom.com on April 2nd, 2024 with no pre-existing user IDs from a data center

Fandom.com appears to be a publisher client of IAS and DoubleVerify, and has installed pre-bid Javascript code from IAS and DoubleVerify on its website.

Progressive insurance ad served by Trade Desk and Index Exchange.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain".

yang tipis dan dahinya yang lebar. Dia biasanya mengolah rambutnya dengan gaya rambut sanggul terbalik dengan pinggiran membingkai kedua sisi wajahnya, dan keningnya terbuka.

Pakaiannya hanya terdiri dari tunik putih berwarna terang dan celana berwarna gelap. Tuniknya memanjang di bawah pinggangnya dan memiliki lengan panjang yang sedikit melewati sikunya. Selain itu, tunik juga memiliki saku kanguru di bagian depan di perutnya. Celana panjangnya sedikit di bawah lutut dan pas untuknya. Dia memakai tas biru yang dia gendong di bahu kanannya, yang membawa grimoire di sisi kirinya. Akhirnya, dia juga memakai sepasang flat kuning berwarna terang untuk alas kakinya.

Sebagai anggota regu Banteng Hitam, Charmy juga mengenakan jubah khas regu. Jubah hitam ini hanya menutupi bagian atas tubuhnya. Ini memiliki hiasan emas dan tudung. Lambang pasukan ... sisi kiri sementara tombol emas yang membuat jubah bersama berada di sisi yang berlawanan ... terlihat dengan pipi memerah.

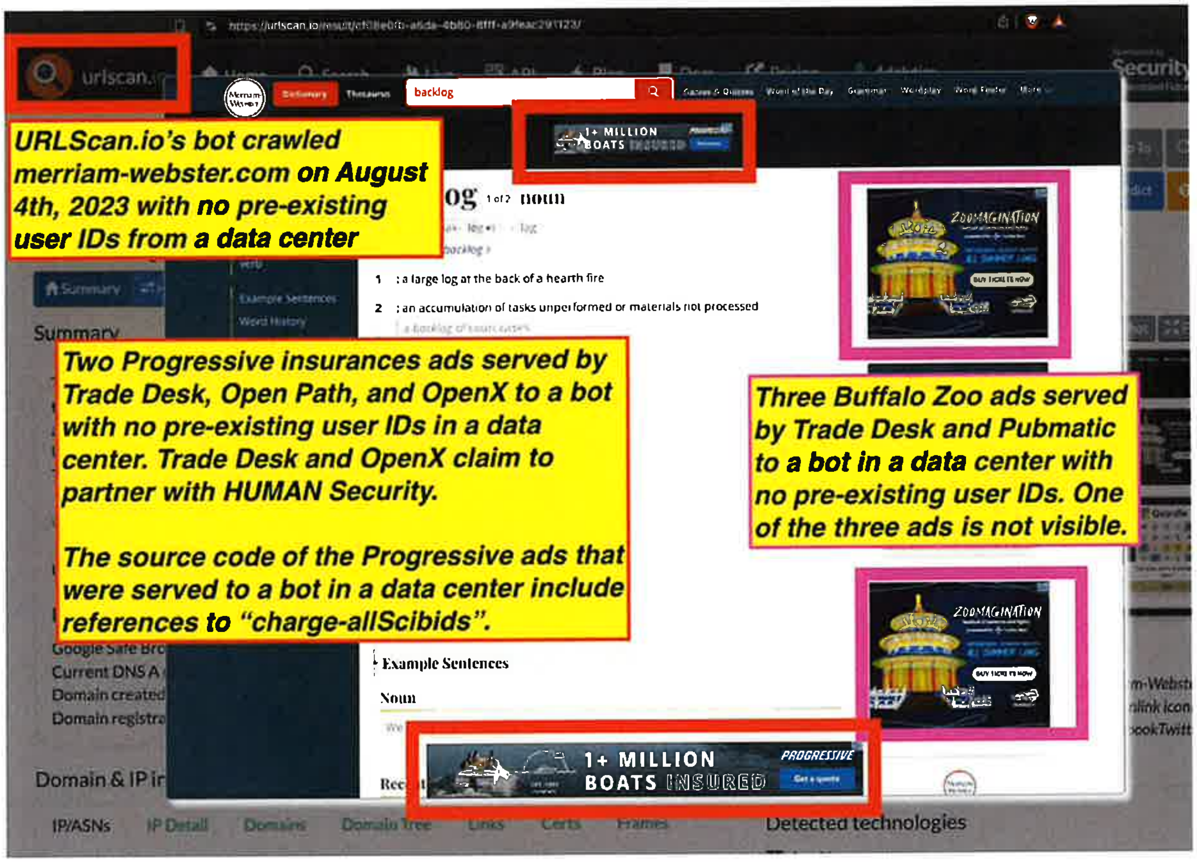
Di pantai, Charmy mengenakan baju renang one-piece biru dan putih.

Ketika dia mengaktifkan Sihir Makanannya, Charmy tumbuh jauh lebih tinggi dan mendapatkan ... lebih dewasa dan tubuh yang berkembang, membuatnya tampak lebih seperti usianya. Dalam bentuk ini, rambutnya tergerai.

Galeri

Screenshot of URLScan.io's bot crawling blackclover.fandom.com on April 2nd, 2024 whilst being shown a Progressive insurance ad that contains references to "charge-allScibids" and "adbrain". The publisher fandom.com appears to have configured the IAS and DoubleVerify publisher optimization tools on its website, and lists IAS and DoubleVerify as "partners" in its media kit for prospective advertisers. Source: https://urlscan.io/result/54af4acf-1183-449d-a939-a79ff4c2df6c/

As another example, two Progressive insurance ads were served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website merriam-webster.com on August 4th, 2023 from a data center. The source code of the Progressive insurance ads includes references to "charge-allScibids".



1 : a large log at the back of a hearth fire

2 : an accumulation of tasks unperformed or materials not processed

URLScan.io's bot crawled merriam-webster.com on August 4th, 2023 with no pre-existing user IDs from a data center

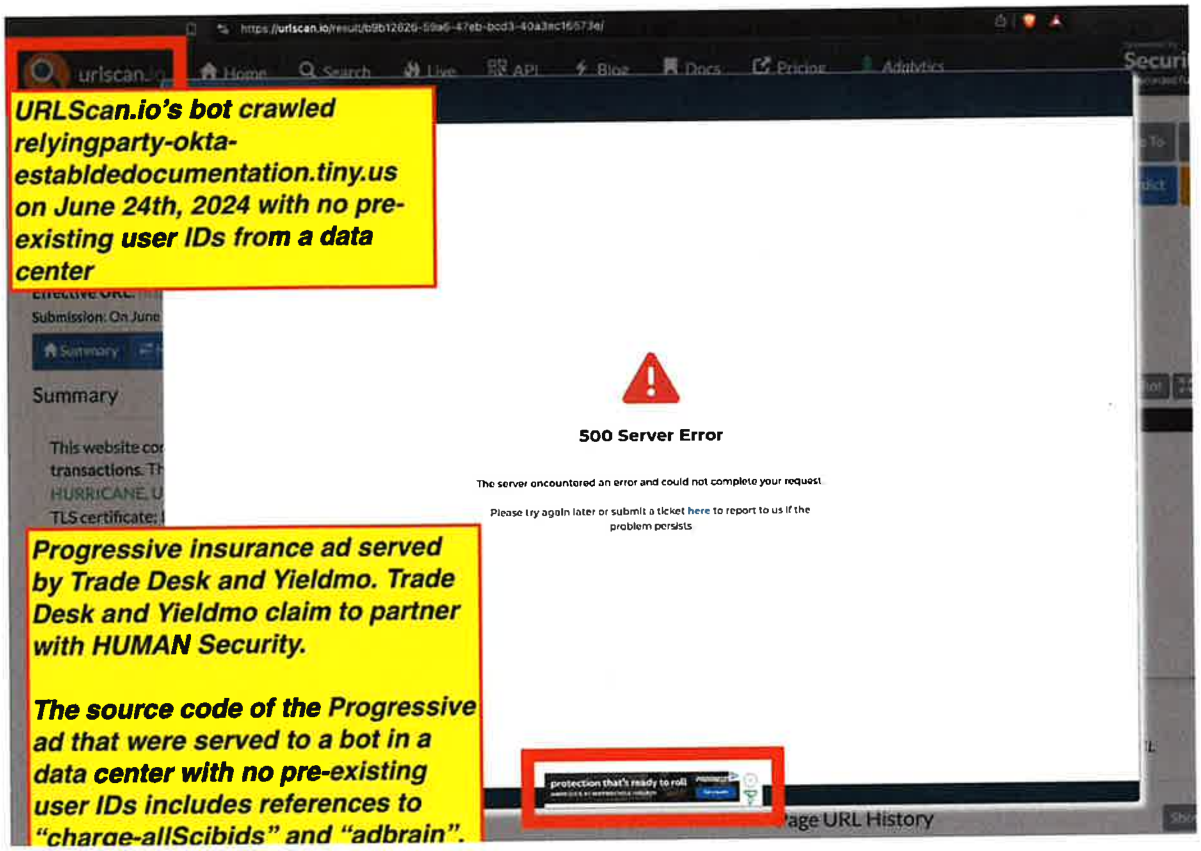
Two Progressive insurances ads served by Trade Desk, Open Path, and OpenX to a bot with no pre-existing user IDs in a data center. Trade Desk and OpenX claim to partner with HUMAN Security.

The source code of the Progressive ads that were served to a bot in a data center include references to "charge-allScibids".

Three Buffalo Zoo ads served by Trade Desk and Pubmatic to a bot in a data center with no pre-existing user IDs. One of the three ads is not visible.

Screenshot of URLScan.io's bot crawling merriam-webster.com on August 4th, 2023 whilst being shown two Progressive insurance ads that contain references to "charge-allScibids". Source: https://urlscan.io/result/cf08e0fb-a6da-4b80-8fff-a9feac291123/

As another example, in the screenshot below one can see a Progressive insurance ad that was served to URLScan.io's bot whilst the bot with no pre-existing user identifiers was crawling the website relyingparty-okta-establdedocumentation.tiny.us on June 24th, 2024 from a data center. The website generated a 500 HTTP status error, meaning the website did not load properly when the bot crawled the page. The source code of the Progressive insurance ad includes references to "charge-allScibids" and "adbrain".


https://urlscan.io/result/b9b12626-59a6-47eb-bcd3-40a3ec16573e/
urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Adalytics
Summary
protection that's ready to roll
Page URL History

URLScan.io's bot crawled relyingparty-okta-establdedocumentation.tiny.us on June 24th, 2024 with no pre-existing user IDs from a data center

500 Server Error

The server encountered an error and could not complete your request

Please try again later or submit a ticket here to report to us if the problem persists

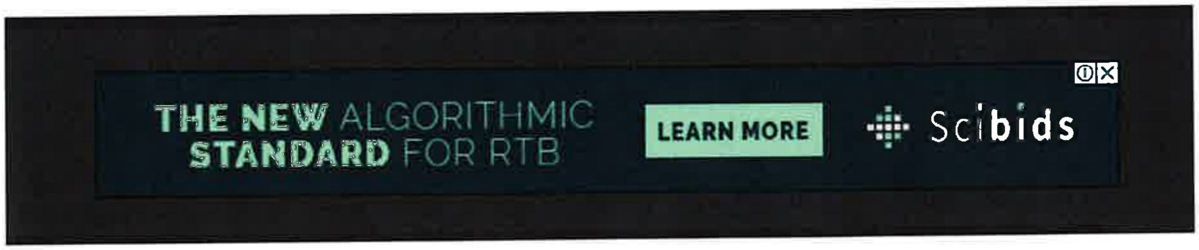
Progressive insurance ad served by Trade Desk and Yieldmo. Trade Desk and Yieldmo claim to partner with HUMAN Security.

The source code of the Progressive ad that were served to a bot in a data center with no pre-existing user IDs includes references to "charge-allScibids" and "adbrain".

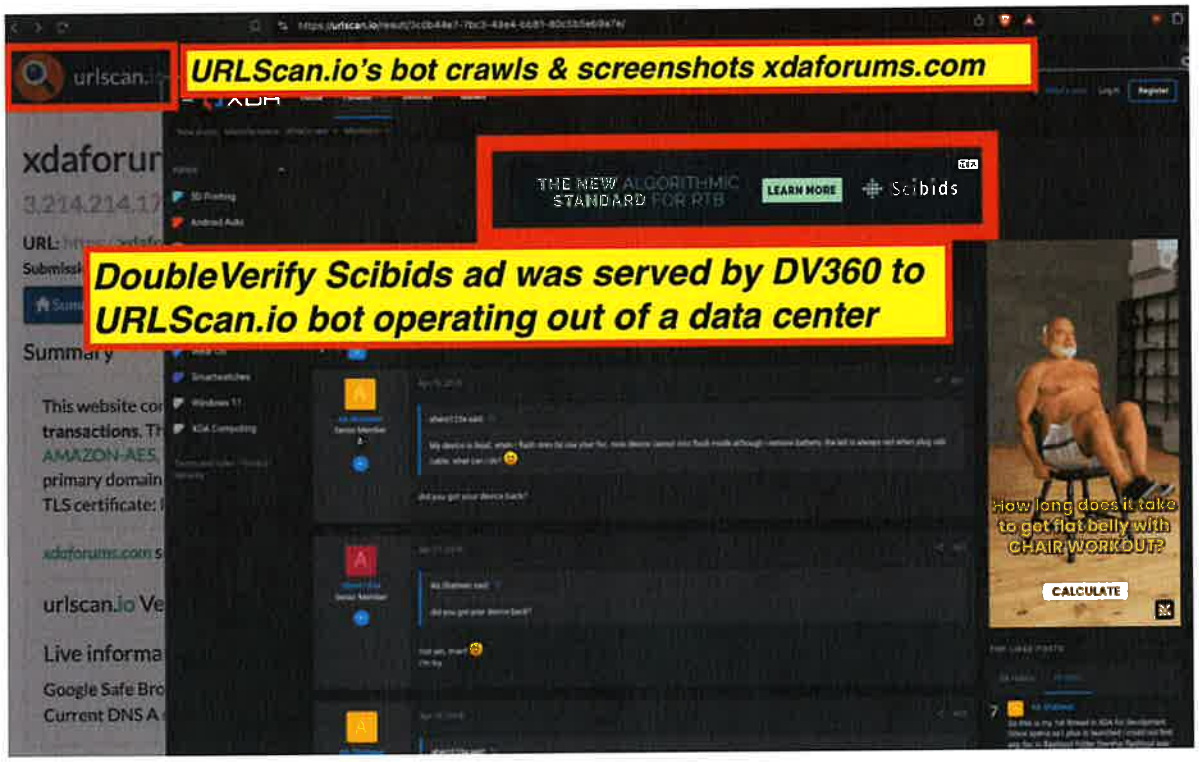
Screenshot of URLScan.io's bot crawling relyingparty-okta-establdedocumentation.tiny.us on June 24th, 2024 whilst being shown two Progressive insurance ads that contain references to "charge-allScibids" and "adbrain". Source: https://urlscan.io/result/b9b12626-59a6-47eb-bcd3-40a3ec16573e/

In addition to potential Scibids' like Progressive having their ads served to bots, there appear to be instances where Scibids own ads for itself were served to bots.

In the screenshot below, one can see an example of a Scibids ads. The Scibids ad says: "The new algorithmic standard for RTB."



On June 24th 2024, the Scibids ad was served by DV360 to a URLScan.io bot operating out of a i3D.net data center IP address in Japan. The URLScan.io bot was crawling the page xdaforums.com. One can see a detailed recording of the page crawl session and the screenshot the bot took of the page - including the Scibids ad - here: https://urlscan.io/result/3c0b44e7-7bc3-49e4-bb81-80c5b5eb9a7e/. One can see the DV360 bid response here: https://urlscan.io/responses/660da871034e80d36a3e0ebfbe1ad9de0838a7548654dafdf476d69346dcb48b/

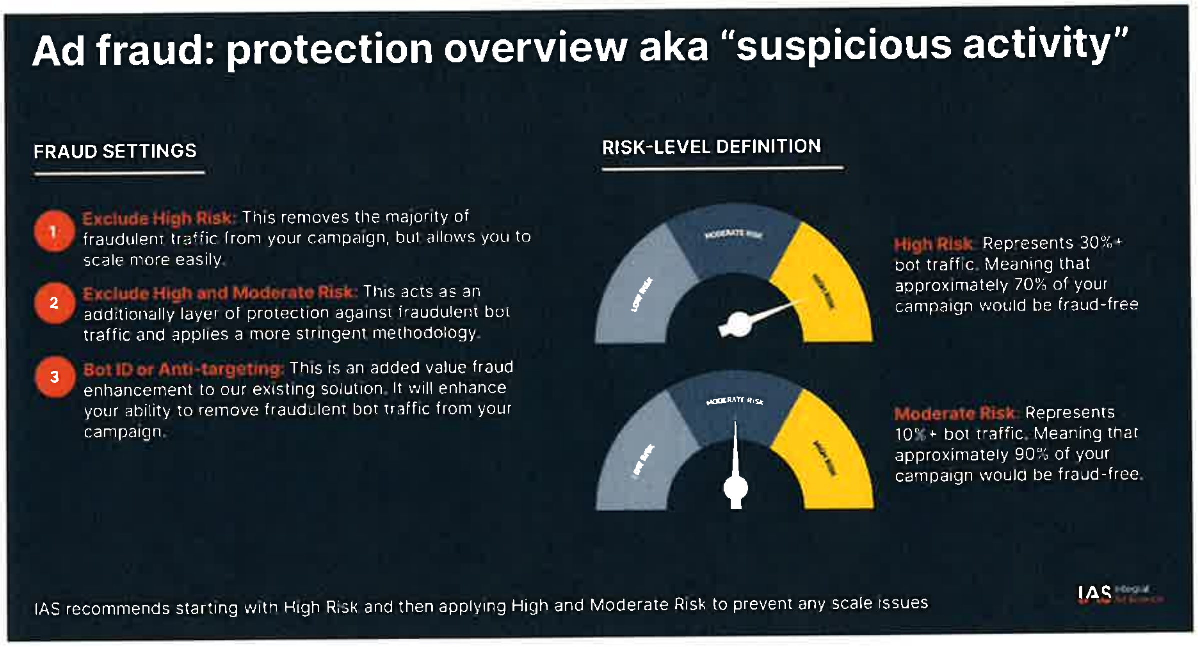

URLScan.io's bot crawls & screenshots xdaforums.com
urlscan.io
xdaforums.com
THE NEW ALGORITHMIC STANDARD FOR RTB
LEARN MORE
Scibids
DoubleVerify Scibids ad was served by DV360 to URLScan.io bot operating out of a data center
How long does it take to get flat belly with CHAIR WORKOUT?
CALCULATE

Screenshot of a DoubleVerify Scibids ad served to a URLScan.io bot operating out of a i3D.net data center in Japan. URLScan.io source - https://urlscan.io/result/3c0b44e7-7bc3-49e4-bb81-80c5b5eb9a7e

Research Results: Brands whose ads include references to "charge-allIntegralQualitySync" or "charge-allIntegralSuspiciousActivity" and had their ads served to bots

Integral Ad Science offers advertisers various pre-bid targeting segments that inform the bidding activity of their programmatic auction bidders and demand side platforms (DSPs).

According to IAS' public documentation, IAS offers a pre-bid segment to prevent ad fraud or "suspicious activity". These segments can help "remove fraudulent bot traffic from your campaign."



Ad fraud: protection overview aka "suspicious activity"

FRAUD SETTINGS

1. **Exclude High Risk:** This removes the majority of fraudulent traffic from your campaign, but allows you to scale more easily.
2. **Exclude High and Moderate Risk:** This acts as an additionally layer of protection against fraudulent bot traffic and applies a more stringent methodology.
3. **Bot ID or Anti-targeting:** This is an added value fraud enhancement to our existing solution. It will enhance your ability to remove fraudulent bot traffic from your campaign.

RISK-LEVEL DEFINITION

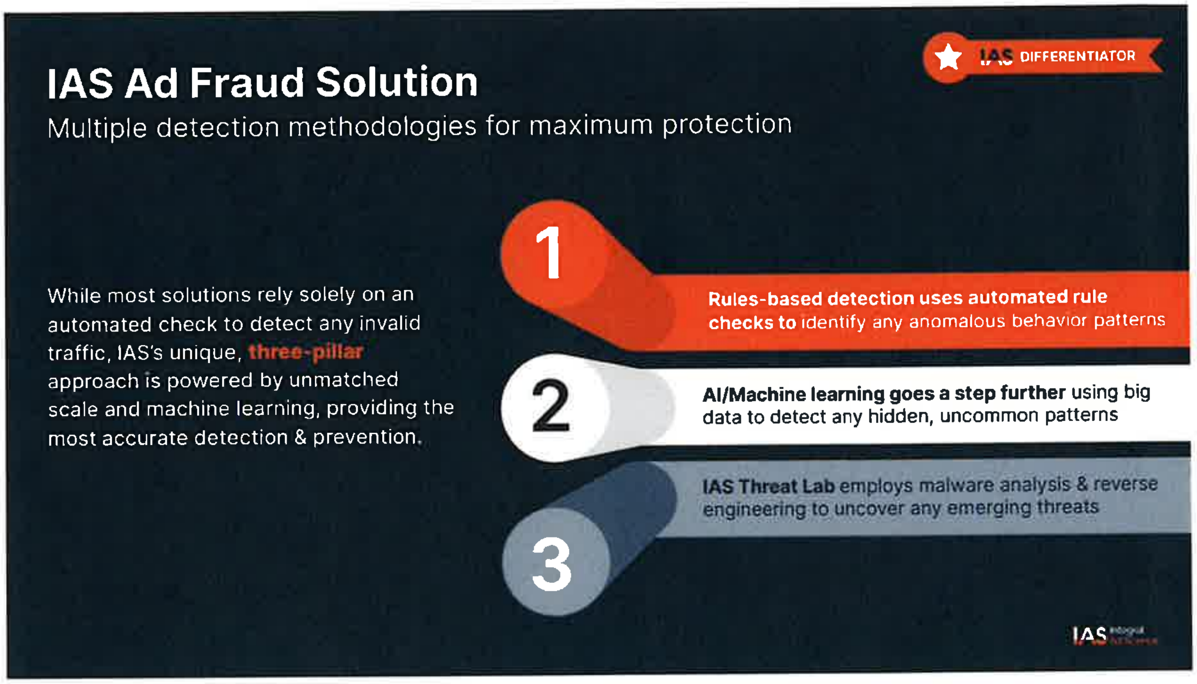
High Risk: Represents 30%+ bot traffic. Meaning that approximately 70% of your campaign would be fraud-free

Moderate Risk: Represents 10%+ bot traffic. Meaning that approximately 90% of your campaign would be fraud-free.

IAS recommends starting with High Risk and then applying High and Moderate Risk to prevent any scale issues

Screenshot of IAS technical documentation, describing IAS "Suspicious Activity" Pre-Bid Segments; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

According to IAS' public documentation, IAS' Ad Fraud Solution utilized multiple detection methodologies for maximum protection. This three-pillar approach is marketed as being "powered by unmatched scale and machine learning, providing the most accurate detection & prevention." The IAS Ad Fraud Solution claims to use "rules-based detection [...] to identify any anomalous behavior patterns", "AI/Machine Learning [...] using big data to detect any hidden, uncommon patterns", and "malware analysis & reverse engineering to uncover any emerging threats."



IAS DIFFERENTIATOR

IAS Ad Fraud Solution

Multiple detection methodologies for maximum protection

While most solutions rely solely on an automated check to detect any invalid traffic, IAS's unique, **three-pillar** approach is powered by unmatched scale and machine learning, providing the most accurate detection & prevention.

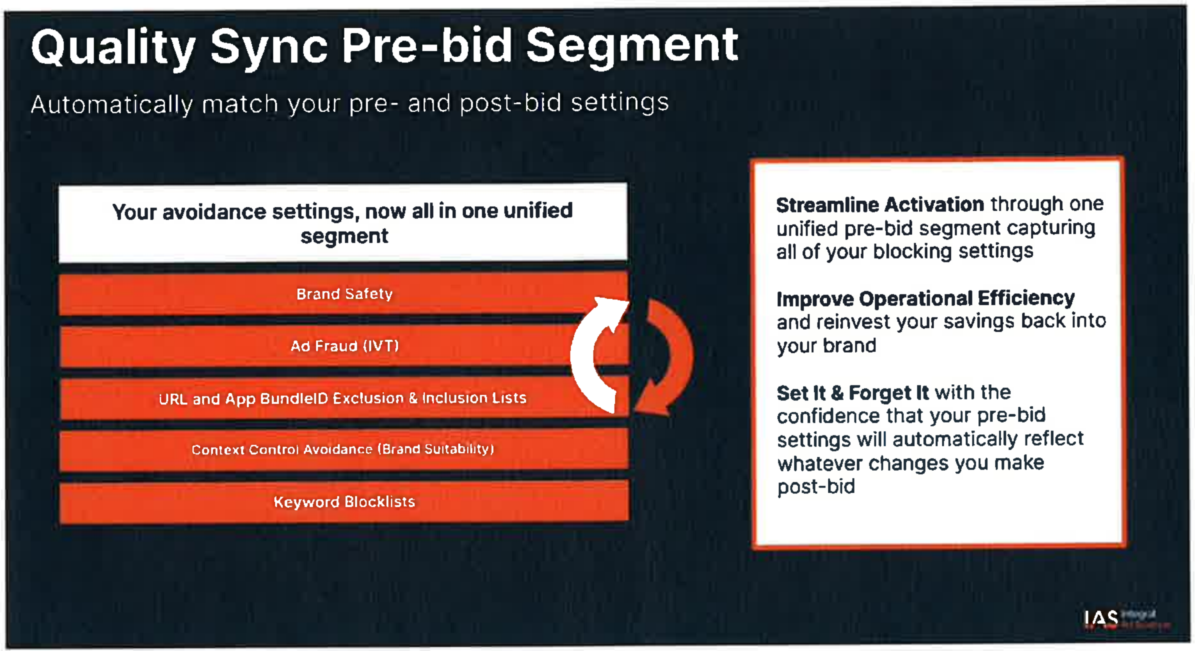
1 **Rules-based detection uses automated rule checks to** identify any anomalous behavior patterns

2 **AI/Machine learning goes a step further** using big data to detect any hidden, uncommon patterns

3 **IAS Threat Lab** employs malware analysis & reverse engineering to uncover any emerging threats

Screenshot of IAS technical documentation, describing IAS Ad Fraud Solution; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

According to IAS' public documentation, IAS offers a "Quality Sync" Pre-bid segment which "automatically matches your pre- and post-bid settings" including "Ad Fraud (IVT)" settings.



Quality Sync Pre-bid Segment

Automatically match your pre- and post-bid settings

Your avoidance settings, now all in one unified segment

- Brand Safety
- Ad Fraud (IVT)
- URL and App BundleID Exclusion & Inclusion Lists
- Context Control Avoidance (Brand Suitability)
- Keyword Blocklists

Streamline Activation through one unified pre-bid segment capturing all of your blocking settings

Improve Operational Efficiency and reinvest your savings back into your brand

Set It & Forget It with the confidence that your pre-bid settings will automatically reflect whatever changes you make post-bid

Screenshot of IAS technical documentation, describing IAS Quality Sync Pre-Bid Segments; Source: https://go.integralads.com/rs/469-VBI-606/images/IAS_Xandr_User_Guide.pdf; Archived: https://perma.cc/93NM-2S2Q

It appears that hundreds of major brands whose ads' source code include references to "charge-allIntegralQualitySync" or "charge-allIntegralSuspiciousActivity" have had their ads served to bots in data centers in the time period ranging from 2017 to 2024. In some cases, brands whose ads included these references were seen as having their ads served to declared bots operating out of known data center IP addresses whose user agent has been on the IAB Tech Lab's Bots and Spiders reference list since 2013.

For example, the Government of DC (the US Capital) had ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the DC Government's ads' source code included references to "charge-allIntegralSuspiciousActivity". For example, the DC Government had its ads served to a declared bot operating out of a known data center IP in November 2023 on the websites jaogata.exblog.jp, maitressreariane.eklablog.com, and worthingcourtblog.com. The DC Government ads were transacted by the Trade Desk Open Path, Index Exchange and Sovrn (f/k/a Federated Media).

As a second example, the British healthcare company Haleon had ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the Haleon ads' source code included references to "charge-allIntegralSuspiciousActivity". For example, Haleon had its advil.com ads served to a declared bot operating out of a known data center IP in November 2023 on the websites themakerista.com, strengthandsunshine.com, and worthingcourtblog.com. The Haleon Advil ads were transacted by Kargo and Mediagrid.

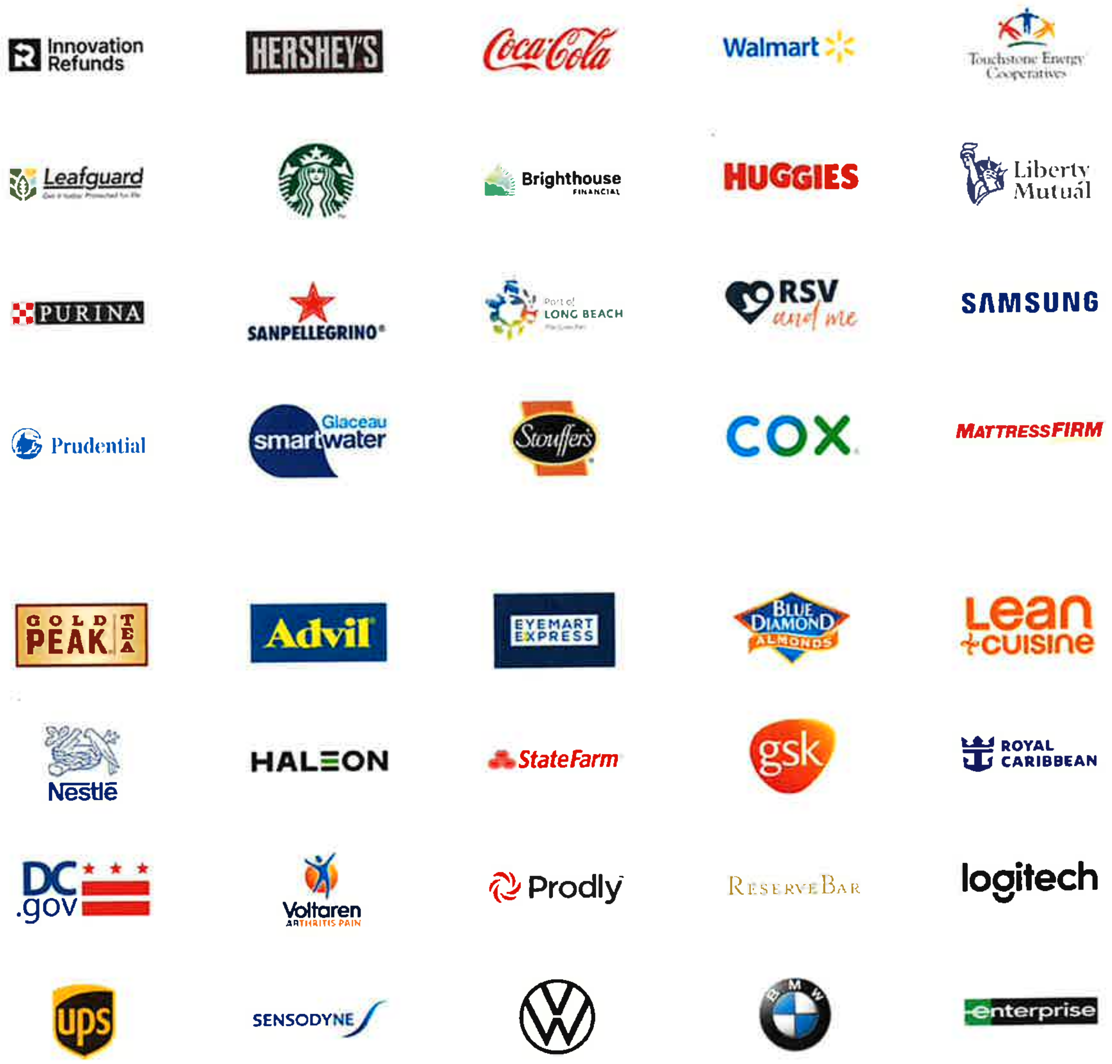
As a third example, Hershey's had ads served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the Hershey's ads' source code included references to "charge-allIntegralQualitySync". For example, Hershey's had its ads served to a declared bot operating out of a known data center IP in March 2024 on the websites bordercolliehealth.com, isavea2z.com, and amyromeu.com. The Hershey's ads that were served to declared bots in data centers were transacted by Trade Desk Open Path, Sharethrough, Index Exchange, GumGum, Yieldmo, Kargo, TrustX, Microsoft Xandr, OpenX, and Teads.

As a fourth example, Kenvue (f/k/a Johnson & Johnson Consumer Health) had ads for Listerine, Tylenol, and Imodium served to declared bots on the IAB Bots List operating out of known data center IPs, wherein the source code for Kenvue's ads' included references to "charge-allIntegralQualitySync". For example, Kenvue had its ads served to a declared bot operating out of a known data center IP in July 2024 on the websites pineapplepaperco.com, thegonegoat.com, and lakelandmom.com. The Kenvue ads that were served to declared bots in data centers were transacted by Index Exchange, ShareThrough, and Reset Digital.

The list of brands whose ads' source code includes references to "charge-allIntegralSuspiciousActivity" or "charge-allIntegralQualitySync", and had their ads served to a declared bot on the IAB Bots List operating out of a known data center IP address included many major brands such as Hersheys, Coca-Cola, Walmart, Starbucks, Kimberly Clark, Liberty Mutual, Nestle, Samsung, Haleon, Cox Communications, State Farm, the Government of DC, UPS, Enterprise car rental, Kenvue, Energizer, CVS, JPMorgan Chase, GSK, Patagonia, Mars, Walgreens, Audi USA, Weight Watchers, USPS, Cigna, Thomson Reuters, and Discover.

A sample list of the brands whose ads were served to declared bots on the IAB Tech Lab's Bots & Spiders list operating out of known data center IP address, and whose ads included references to "charge-allIntegralSuspiciousActivity" or "charge-allIntegralQualitySync" is shown below.

Brands whose ads referenced "charge-allIntegralQualitySync" or "charge-allIntegralSuspiciousActivity" & were served to declared bots (listed on the IAB Bots & Spiders List since 2013) operating from known data center IPs



CHUCK E. CHEESE'S
Qlik
Simply beverages
Rosetta Stone
IMDb
TYLENOL
He Gets Us
MICHIGAN ECONOMIC DEVELOPMENT CORPORATION
Imodium
KitKat
GLOBUS
NESCAFÉ
UNIVERSITY OF DETROIT MERCY
sondermind Therapy Works
Energizer
vitaminwater
SONOMA-CUTRER
Sprite
LISTERINE

JPMORGAN CHASE & CO.
Scott
John Hancock
Harbor Capital
Bekaert
DTS Teach Truth. Love Well.
CVS
VIRGINIA BEACH LIVE THE LIFE
XEOMIN IncobotulinumtoxinA
Nucala (mepolizumab)
GSK
UP Union Pearson Express
NEW ORLEANS
MINI
Benlysta (belimumab)
SOKA UNIVERSITY OF AMERICA
SNICKERS
PING
jiffy lube
Bally SPORTS
LEUKEMIA & LYMPHOMA SOCIETY

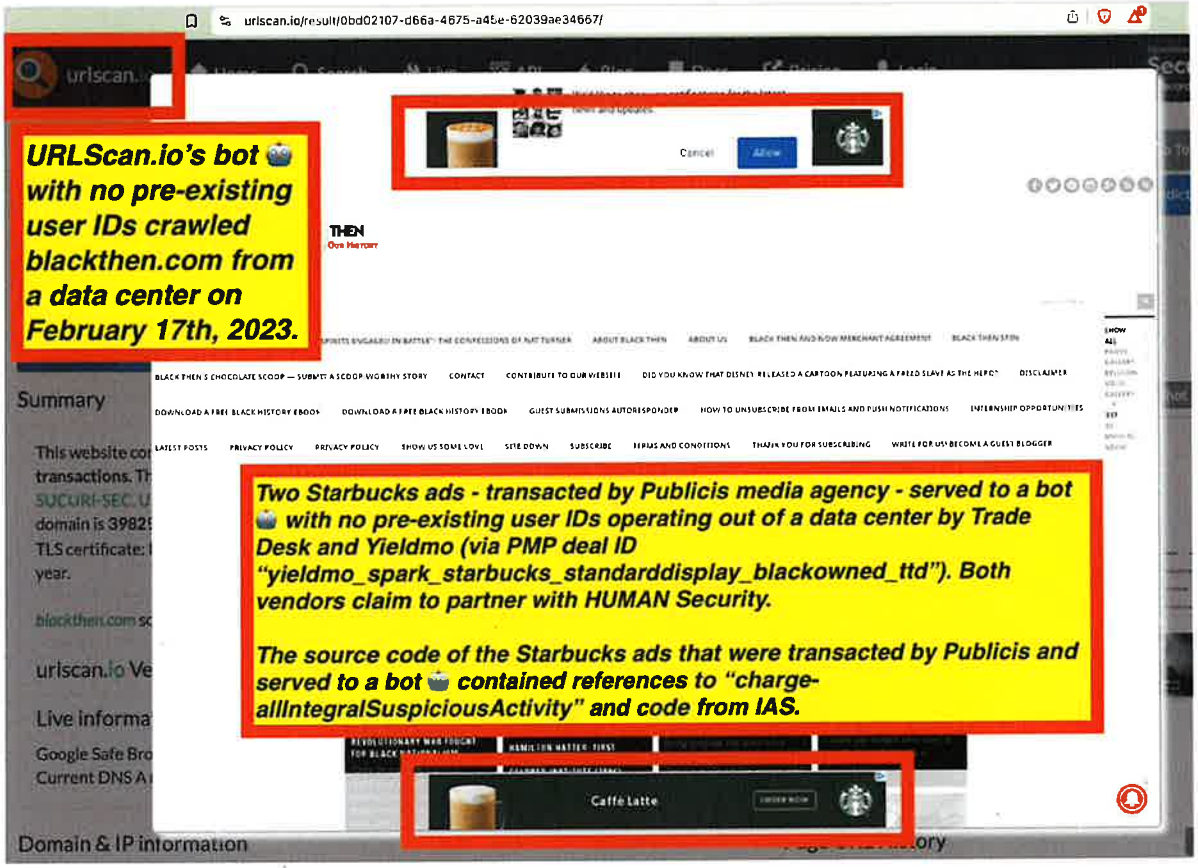
WYNDHAM HOTELS & RESORTS
EVOSHIELD
UNITED STATES POSTAL SERVICE
JUST
BERMUDA GoToBermuda.com
R
COLORADO STATE UNIVERSITY GLOBAL CAMPUS
Walmart
cigna healthcare
BEXSERO
TREK
Carnegie Mellon University
VITAL PROTEINS
CIRCLE
YOSEMITE
A/C PRO
VICTORIA'S SECRET
All-Clad METALCRAFTERS
care.
WINTERTHUR MUSEUM, GARDEN & LIBRARY

Emergen-C
patagonia
Room&Board
elf
IALottery Woo Hoo for You
MGM RESORTS INTERNATIONAL
SHORAI
VISIT Myrtle Beach SOUTH CAROLINA
Shipt
Walgreens
OPEN FARM
Lubriderm dermatologist developed
Nu Finish
Audi
weight watchers
OUTBACK STEAKHOUSE
FUJIFILM
THERAFLU
AAA
NATERNAL

That's WY
Thomson Reuters
Pinterest
Martin Luther King, Jr Community Hospital
MUMM NAPA
MURDOCH'S
Nature's Way
Lactaid
KOA
NUTRISH
Operation Smile
XIAFLEX
Poise
DAVID YURMAN
Imperial
HOLLISTER
GO RVING
FOOD LION
Schreiber
SiteOne
Dramamine
tajín
Terry Naturally Vitamins
DISCOVER

Secondarily, many brands whose ads' source code includes references to "charge-allIntegralSuspiciousActivity" and "charge-allIntegralQualitySync" appear to have had their ads served to URLScan.io's bots.

As an example, in the screenshot below one can see two ads for Starbucks that were served to URLScan.io's bot whilst the bot was crawling blackthen.com from a data center on February 17th, 2023. The Starbucks ads - which appear to have been transacted by Publicis media agency, Trade Desk, and Yieldmo SSP - include references to "charge-allIntegralSuspiciousActivity" and code from IAS.



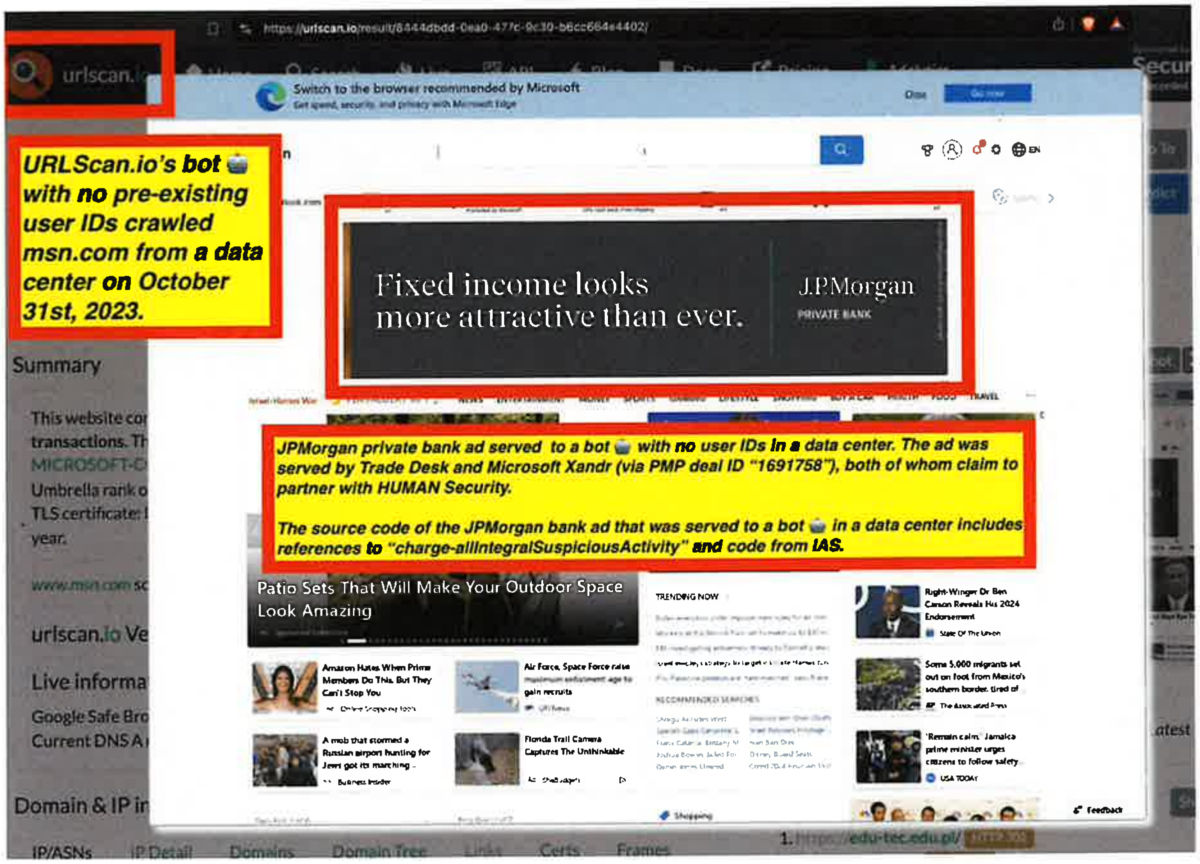
URLScan.io's bot 🤖 with no pre-existing user IDs crawled blackthen.com from a data center on February 17th, 2023.

Two Starbucks ads - transacted by Publicis media agency - served to a bot 🤖 with no pre-existing user IDs operating out of a data center by Trade Desk and Yieldmo (via PMP deal ID "yieldmo_spark_starbucks_standarddisplay_blackowned_ttd"). Both vendors claim to partner with HUMAN Security.

The source code of the Starbucks ads that were transacted by Publicis and served to a bot 🤖 contained references to "charge-allIntegralSuspiciousActivity" and code from IAS.

Two Starbucks ads transacted by Publicis, Trade Desk, and Yieldmo to a bot in a data center. The source code of the Starbucks ads include references to "charge-allIntegralSuspiciousActivity" and source code from IAS. Source: https://urlscan.io/result/0bd02107-d66a-4675-a45e-62039ae34667/

As another example, in the screenshot below one can see an ad for JPMorgan Chase that was served to URLScan.io's bot whilst the bot was crawling blackthen.com from a data center on October 31st, 2023. The JPMorgan Chase ad appears to include references to "charge-allIntegralSuspiciousActivity" and code from IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled msn.com from a data center on October 31st, 2023.

JPMorgan private bank ad served to a bot 🤖 with no user IDs in a data center. The ad was served by Trade Desk and Microsoft Xandr (via PMP deal ID "1691758"), both of whom claim to partner with HUMAN Security.

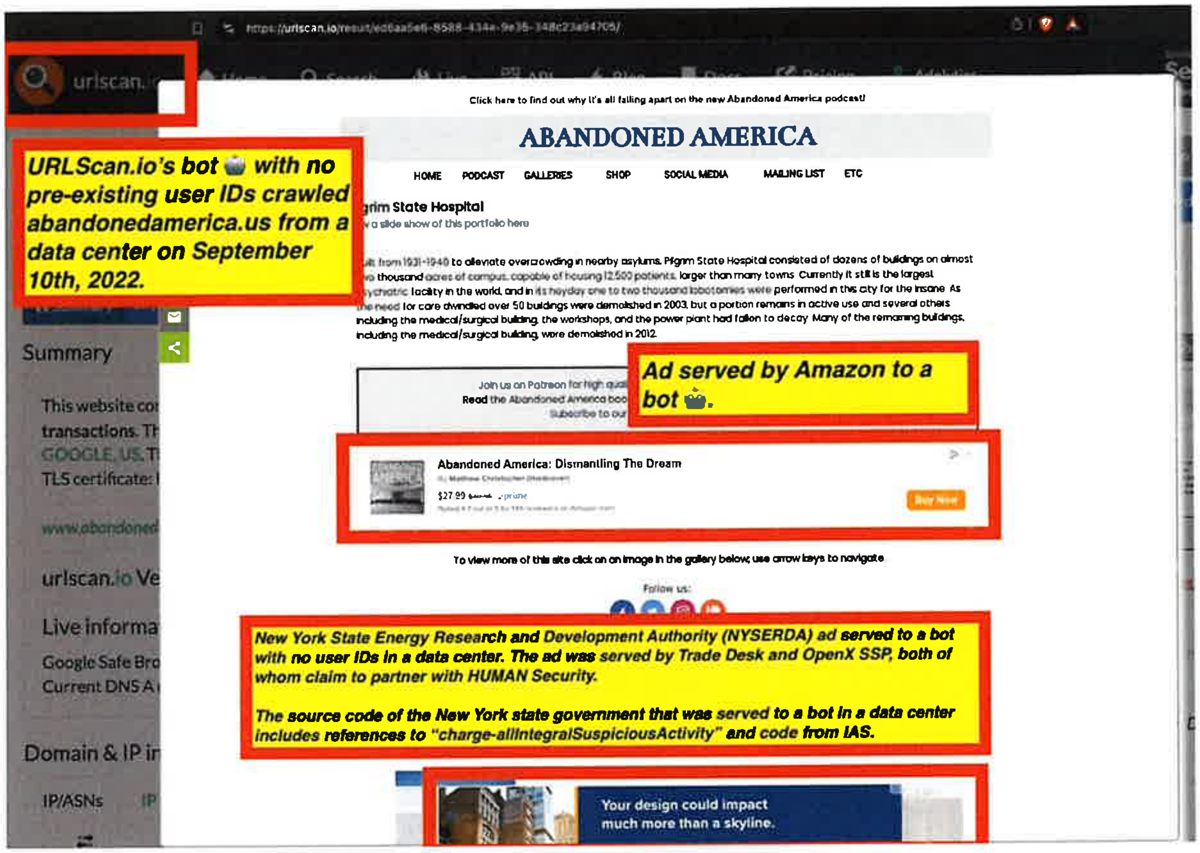
The source code of the JPMorgan bank ad that was served to a bot 🤖 in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

https://urlscan.io/result/8444dbdd-0ea0-477c-9c30-b6cc664e4402/
urlscan.io
Switch to the browser recommended by Microsoft
Fixed income looks more attractive than ever.
J.P.Morgan
PRIVATE BANK
Summary
Patio Sets That Will Make Your Outdoor Space Look Amazing
TRENDING NOW
Amazon Hates When Prime Members Do This, But They Can't Stop You
Air Force, Space Force raise maximum enlistment age to gain recruits
A mob that stormed a Russian airport hunting for Jews got its marching
Florida Trail Camera Captures The Unthinkable
Right-Winger Dr Ben Carson Reveals His 2024 Endorsement
Some 5,000 migrants set out on foot from Mexico's southern border, tired of
'Remain calm,' Jamaica prime minister urges citizens to follow safety
urlscan.io Verdict
Live information
Google Safe Browsing
Current DNS A
Domain & IP information
IP/ASNs
IP Detail
Domains
Domain Tree
Links
Certs
Frames
1. https://edu-tec.edu.pl/

URLScan.io's bot 🤖 with no pre-existing user IDs crawled msn.com from a data center on October 31st, 2023. JPMorgan private bank ad served to a bot 🤖 with no user IDs in a data center. The ad was served by Trade Desk and Microsoft Xandr (via PMP deal ID "1691758"), both of whom claim to partner with HUMAN Security. The source code of the JPMorgan bank ad that was served to a bot 🤖 in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

Source: https://urlscan.io/result/8444dbdd-0ea0-477c-9c30-b6cc664e4402/

As another example, in the screenshot below one can see an ad for the New York State Energy Research and Development Authority (NYSERDA), a New York state government agency, that was served to URLScan.io's bot whilst the bot was crawling abandonedamerica.us from a data center on September 10th, 2022. The New York state government ad appears to include references to "charge-allIntegralSuspiciousActivity" and code from IAS.



Click here to find out why it's all falling apart on the new Abandoned America podcast!

ABANDONED AMERICA

HOME PODCAST GALLERIES SHOP SOCIAL MEDIA MAILING LIST ETC

grim State Hospital

a slide show of this portfolio here

lt from 1931-1940 to alleviate overcrowding in nearby asylums. Pilgrim State Hospital consisted of dozens of buildings on almost o thousand acres of campus, capable of housing 12,500 patients, larger than many towns. Currently it still is the largest ychiatric facility in the world, and in its heyday one to two thousand lobotomies were performed in this city for the insane. As the need for care dwindled over 50 buildings were demolished in 2003, but a portion remains in active use and several others including the medical/surgical building, the workshops, and the power plant had fallen to decay. Many of the remaining buildings, including the medical/surgical building, were demolished in 2012.

Join us on Patreon for high qua
Read the Abandoned America boo
Subscribe to our

Abandoned America: Dismantling The Dream
By Matthew Christopher (Hardcover)
$27.99 prime
Buy Now

To view more of this site click on an image in the gallery below; use arrow keys to navigate

Follow us:

Your design could impact much more than a skyline.

URLScan.io's bot 🤖 with no pre-existing user IDs crawled abandonedamerica.us from a data center on September 10th, 2022.

Ad served by Amazon to a bot 🤖.

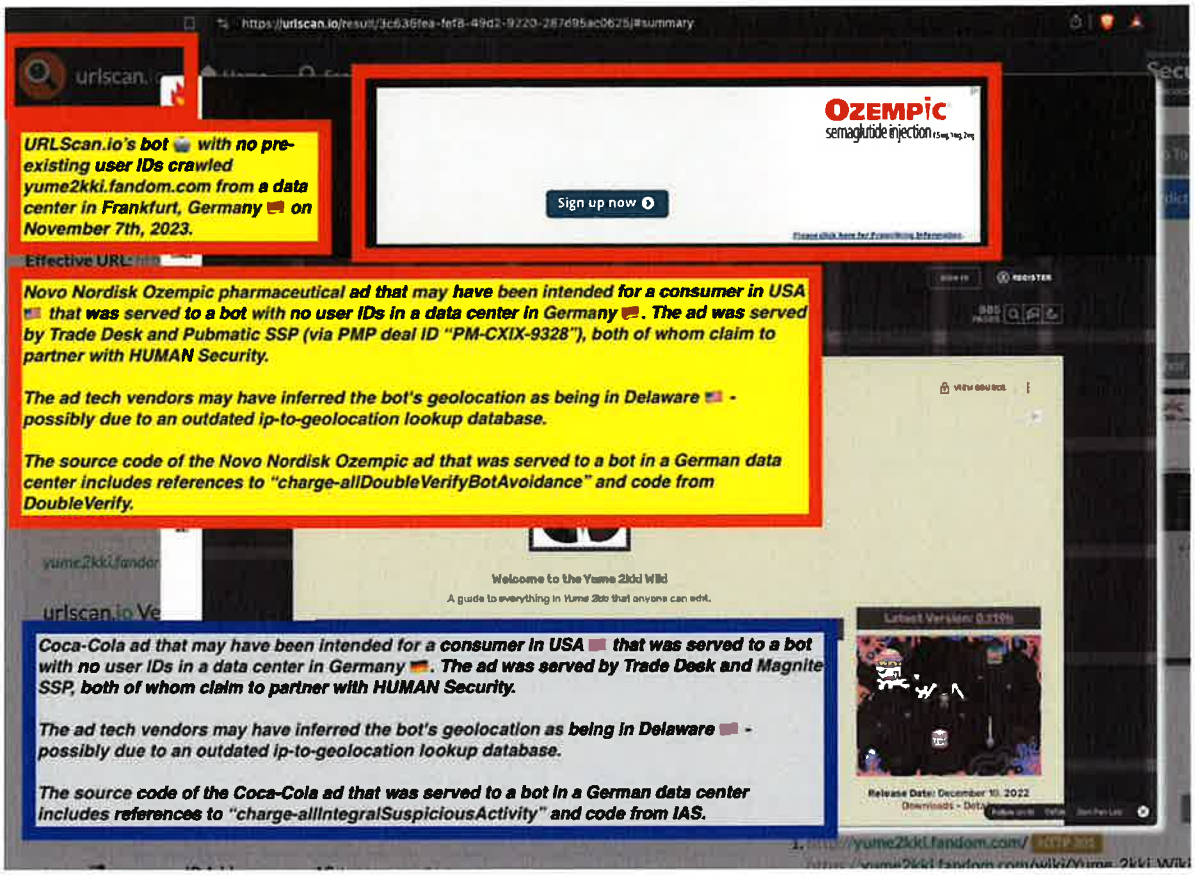
New York State Energy Research and Development Authority (NYSERDA) ad served to a bot with no user IDs in a data center. The ad was served by Trade Desk and OpenX SSP, both of whom claim to partner with HUMAN Security.

The source code of the New York state government that was served to a bot in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

URLScan.io's bot 🤖 with no pre-existing user IDs crawled abandonedamerica.us from a data center on September 10th, 2022. Ad served by Amazon to a bot 🤖. New York State Energy Research and Development Authority (NYSERDA) ad served to a bot with no user IDs in a data center. The ad was served by Trade Desk and OpenX SSP, both of whom claim to partner with HUMAN Security. The source code of the New York state government that was served to a bot in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

Source: https://urlscan.io/result/ed6aa5e6-8588-434e-9e36-348c23a94705/

As another example, an ad for Coca-cola was served to URLScan.io's bot whilst the bot was crawling yume2kki.fandom.com from a data center on November 7th, 2023. The Coca-cola ad appears to include references to "charge-allIntegralSuspiciousActivity" and code from IAS.


https://urlscan.io/result/3c636fea-fef8-49d2-9220-287d95ac0625/#summary
urlscan.
OZEMPIC
semaglutide injection
Sign up now
Effective URL:
Welcome to the Yume 2kki Wiki
A guide to everything in Yume 2kki that anyone can edit.
Latest Version: 0.119h
Release Date: December 10, 2022
yume2kki.fandom.com
urlscan.io Ve
https://yume2kki.fandom.com/

URLScan.io's bot 🤖 with no pre-existing user IDs crawled yume2kki.fandom.com from a data center in Frankfurt, Germany 🇩🇪 on November 7th, 2023.

Novo Nordisk Ozempic pharmaceutical ad that may have been intended for a consumer in USA 🇺🇸 that was served to a bot with no user IDs in a data center in Germany 🇩🇪. The ad was served by Trade Desk and Pubmatic SSP (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Delaware 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

The source code of the Novo Nordisk Ozempic ad that was served to a bot in a German data center includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify.

Coca-Cola ad that may have been intended for a consumer in USA 🇺🇸 that was served to a bot with no user IDs in a data center in Germany 🇩🇪. The ad was served by Trade Desk and Magnite SSP, both of whom claim to partner with HUMAN Security.

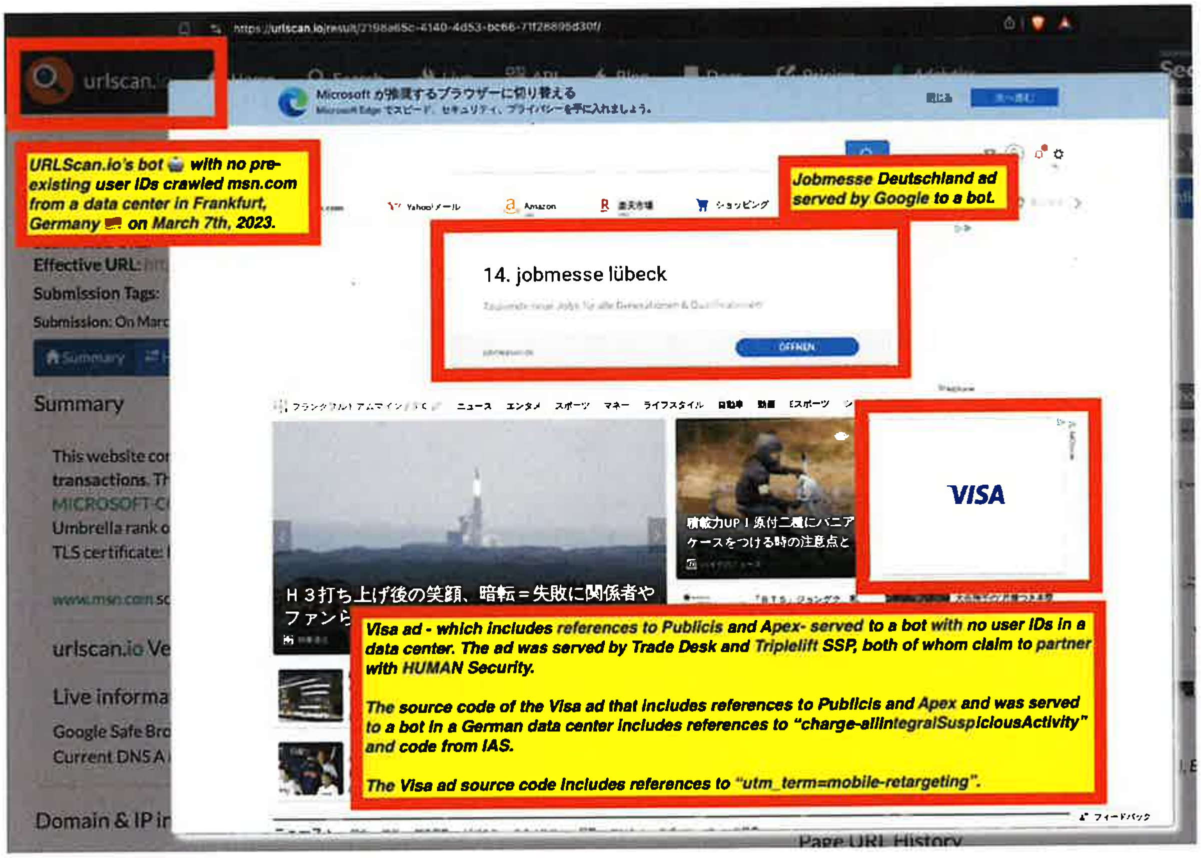
The ad tech vendors may have inferred the bot's geolocation as being in Delaware 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

The source code of the Coca-Cola ad that was served to a bot in a German data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

URLScan.io's bot 🤖 with no pre-existing user IDs crawled yume2kki.fandom.com from a data center in Frankfurt, Germany DE on November 7th, 2023. Novo Nordisk Ozempic pharmaceutical ad that may have been intended for a consumer in USA US that was served to a bot with no user IDs in a data center in Germany DE. The ad was served by Trade Desk and Pubmatic SSP (via PMP deal ID "PM-CXIX-9328"), both of whom claim to partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Delaware US - possibly due to an outdated ip-to-geolocation lookup database. The source code of the Novo Nordisk Ozempic ad that was served to a bot in a German data center includes references to "charge-allDoubleVerifyBotAvoidance" and code from DoubleVerify. Coca-Cola ad that may have been intended for a consumer in USA US that was served to a bot with no user IDs in a data center in Germany DE. The ad was served by Trade Desk and Magnite SSP, both of whom claim to partner with HUMAN Security. The ad tech vendors may have inferred the bot's geolocation as being in Delaware US - possibly due to an outdated ip-to-geolocation lookup database. The source code of the Coca-Cola ad that was served to a bot in a German data center includes references to “charge-allIntegralSuspiciousActivity” and code from IAS.

Source: https://urlscan.io/result/3c636fea-fef8-49d2-9220-287d95ac0625/

As another example, an ad for Visa was served to URLScan.io’s bot whilst the bot was crawling msn.com from a data center on March 7th, 2023. The Visa ad appears to include references to Publicis Apex, and to “charge-allIntegralSuspiciousActivity” and code from IAS.


https://urlscan.io/result/2198a65c-4140-4d53-bc66-71f28895d30f/
urlscan.io
Microsoft が推奨するブラウザーに切り替える
Effective URL:
Submission Tags:
Submission: On Marc
Summary
14. jobmesse lübeck
OFFNEN
VISA
H３打ち上げ後の笑顔、暗転＝失敗に関係者や ファン
urlscan.io Ve
Live informa
Domain & IP in
Page URL History

URLScan.io’s bot 🤖 with no pre-existing user IDs crawled msn.com from a data center in Frankfurt, Germany 🇩🇪 on March 7th, 2023.

Jobmesse Deutschland ad served by Google to a bot.

Visa ad - which includes references to Publicis and Apex- served to a bot with no user IDs in a data center. The ad was served by Trade Desk and Triplelift SSP, both of whom claim to partner with HUMAN Security.

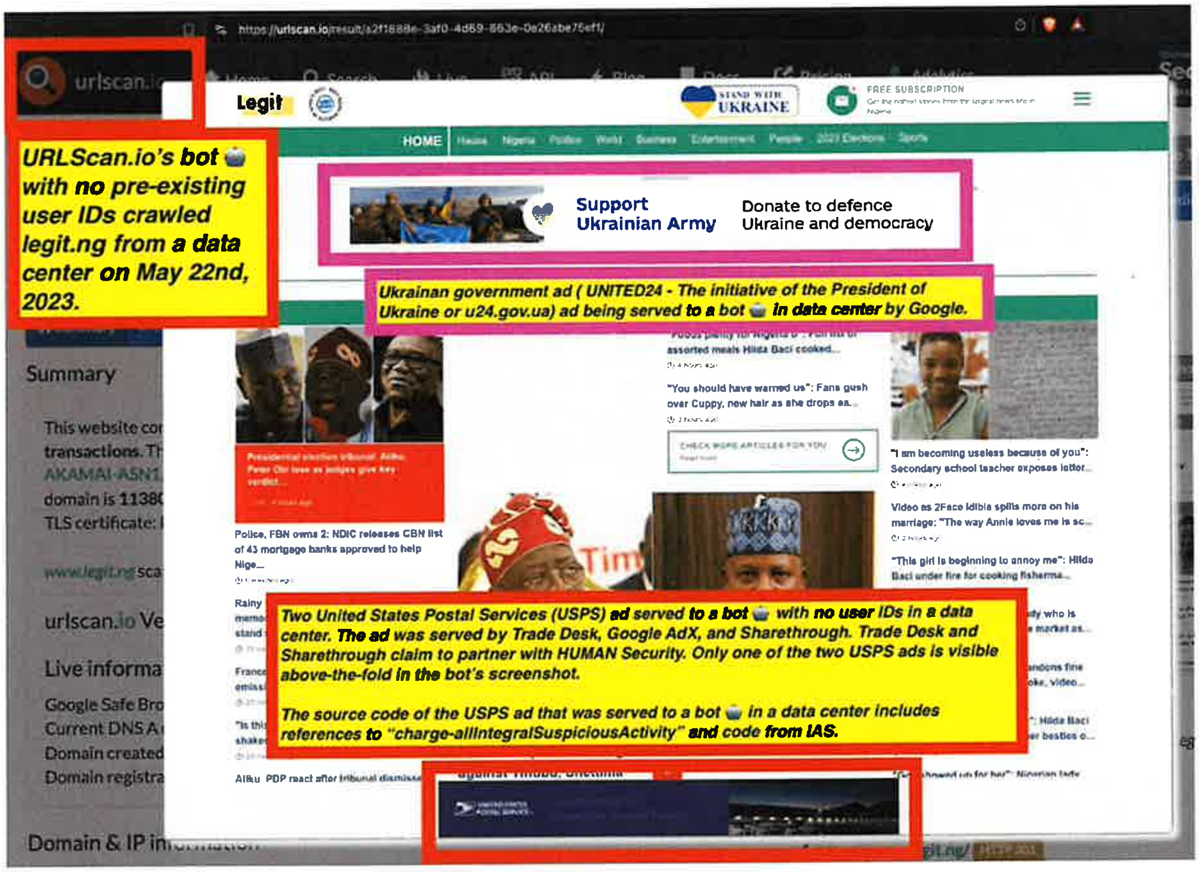
The source code of the Visa ad that includes references to Publicis and Apex and was served to a bot in a German data center includes references to “charge-allIntegralSuspiciousActivity” and code from IAS.

The Visa ad source code includes references to “utm_term=mobile-retargeting”.

URLScan.io’s bot 🤖 with no pre-existing user IDs crawled msn.com from a data center in Frankfurt, Germany DE on March 7th, 2023. Visa ad - which includes references to Publicis and Apex- served to a bot with no user IDs in a data center. The ad was served by Trade Desk and Triplelift SSP, both of whom claim to partner with HUMAN Security. The source code of the Visa ad that includes references to Publicis and Apex and *was served to a bot in a German data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS. The Visa ad source code includes references to "utm_term=mobile-retargeting".*

Source: https://urlscan.io/result/2198a65c-4140-4d53-bc66-71f28895d30f/#summary

As another example, an ad for the United States Postal Service (USPS) was served to URLScan.io's bot whilst the bot was crawling legit.ng from a data center on May 22nd, 2023. The USPS ad appears to include references to "charge-allIntegralSuspiciousActivity" and code from IAS.



URLScan.io's bot 🤖 with no pre-existing user IDs crawled legit.ng from a data center on May 22nd, 2023.

Ukrainian government ad (UNITED24 - The initiative of the President of Ukraine or u24.gov.ua) ad being served to a bot 🤖 in data center by Google.

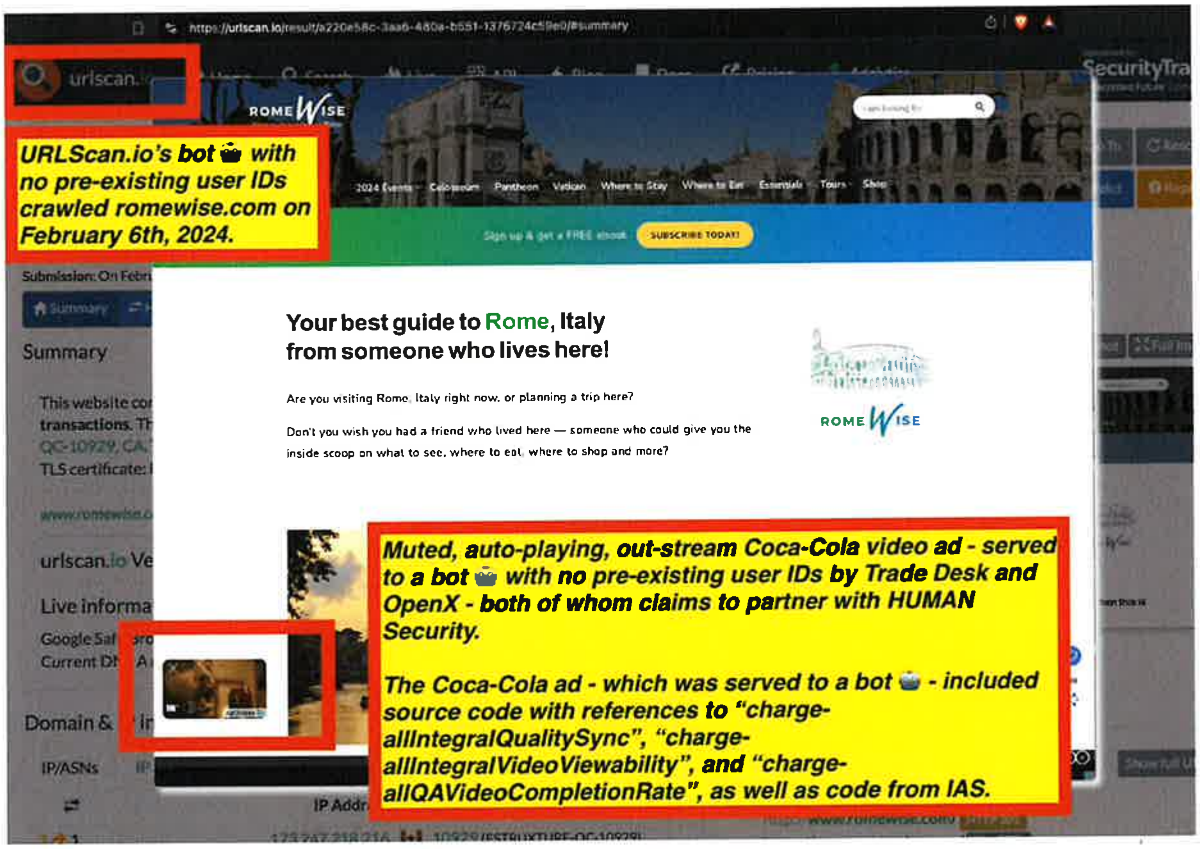
Two United States Postal Services (USPS) ad served to a bot 🤖 with no user IDs in a data center. The ad was served by Trade Desk, Google AdX, and Sharethrough. Trade Desk and Sharethrough claim to partner with HUMAN Security. Only one of the two USPS ads is visible above-the-fold in the bot's screenshot.

The source code of the USPS ad that was served to a bot 🤖 in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

URLScan.io's bot 🤖 with no pre-existing user IDs crawled legit.ng from a data center on May 22nd, 2023. Ukrainian government ad (UNITED24 - The initiative of the President of Ukraine or u24.gov.ua) ad being served to a bot 🤖 in data center by Google. Two United States Postal Services (USPS) ads served to a bot 🤖 with no user IDs in a data center. The ad was served by Trade Desk, Google AdX, and Sharethrough. Trade Desk *and Sharethrough claim to partner with HUMAN Security. Only one of the two USPS ads is visible above-the-fold in the bot's screenshot. The source code of the USPS ad that was served to a bot 🤖 in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.*

Source: https://urlscan.io/result/a2f1888e-3af0-4d69-863e-0e26abe75ef1/

As another example, a muted, auto-playing, out-stream video ad for Coca-cola was served to URLScan.io's bot whilst the bot was crawling romewise.com from a data center on February 6th, 2024. The Coca-cola ad appears to include references to "charge-allIntegralQualitySync", "charge-allIntegralVideoViewability", and "charge-allQAVideoCompletionRate", and code from IAS.



urlscan.io
ROME WISE
2024 Events · Colosseum · Pantheon · Vatican · Where to Stay · Where to Eat · Essentials · Tours · Shop
Sign up & get a FREE ebook
SUBSCRIBE TODAY!
Summary

URLScan.io's bot 🤖 with no pre-existing user IDs crawled romewise.com on February 6th, 2024.

Your best guide to Rome, Italy from someone who lives here!

Are you visiting Rome, Italy right now, or planning a trip here?

Don't you wish you had a friend who lived here — someone who could give you the inside scoop on what to see, where to eat, where to shop and more?

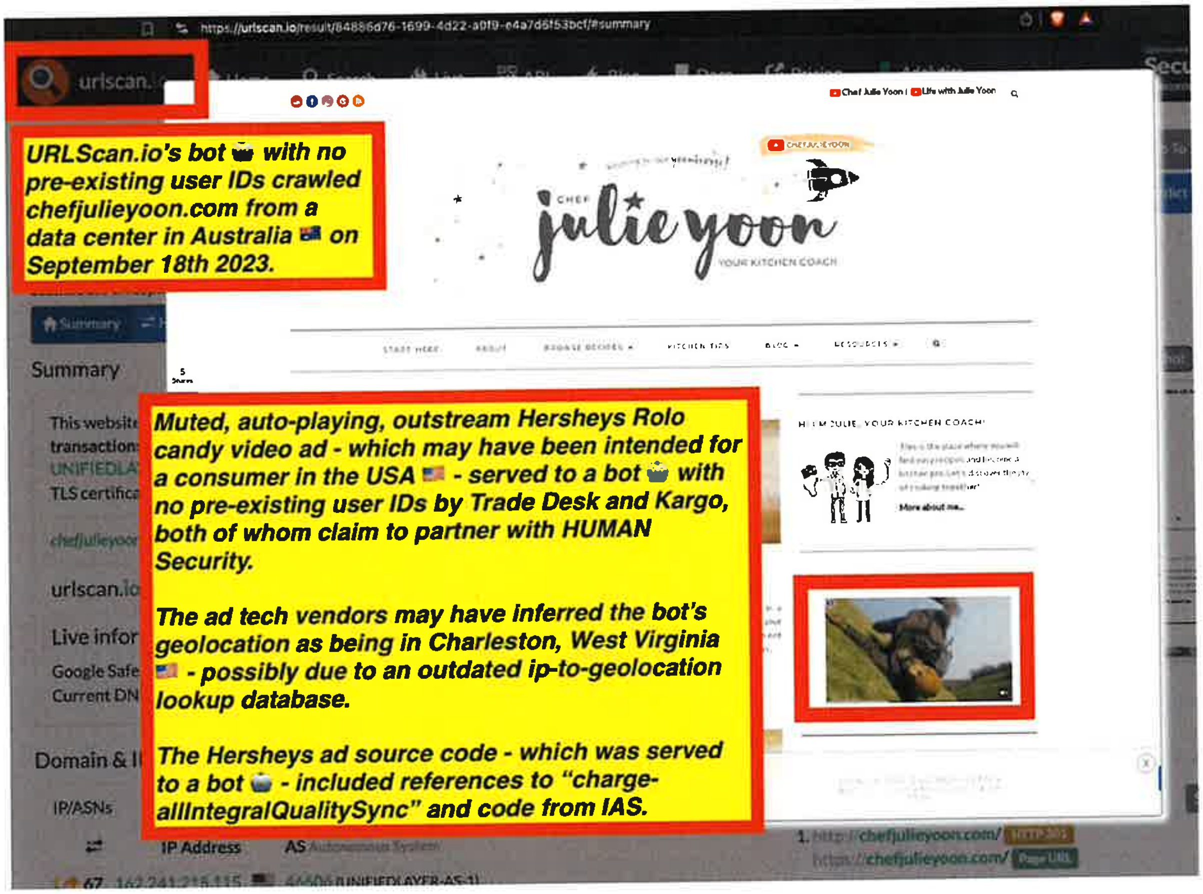
Muted, auto-playing, out-stream Coca-Cola video ad - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and OpenX - both of whom claims to partner with HUMAN Security.

The Coca-Cola ad - which was served to a bot 🤖 - included source code with references to "charge-allIntegralQualitySync", "charge-allIntegralVideoViewability", and "charge-allQAVideoCompletionRate", as well as code from IAS.

A Coca-Cola video ad that was served to URLScan.io's bot. The source code of the Coca-Cola ad appears to contain references to "charge-

allIntegralQualitySync". Source: https://urlscan.io/result/a220e58c-3aa6-480a-b551-1376724c59e0/#summary

As another example, a muted, auto-playing, out-stream video ad for Hershey's Rolo candy was served to URLScan.io's bot whilst the bot was crawling chefjulieyoon.com from a data center in Australia on September 18th, 2023. The Hershey's ad appears to include references to "charge-allIntegralQualitySync" and code from IAS.


https://urlscan.io/result/84886d76-1699-4d22-a0f9-e4a7d6f53bcf/#summary
urlscan.
Summary
chef julie yoon
YOUR KITCHEN COACH
HI I'M JULIE, YOUR KITCHEN COACH!
1. https://chefjulieyoon.com/
https://chefjulieyoon.com/
IP Address
AS

URLScan.io's bot 🤖 with no pre-existing user IDs crawled chefjulieyoon.com from a data center in Australia 🇦🇺 on September 18th 2023.

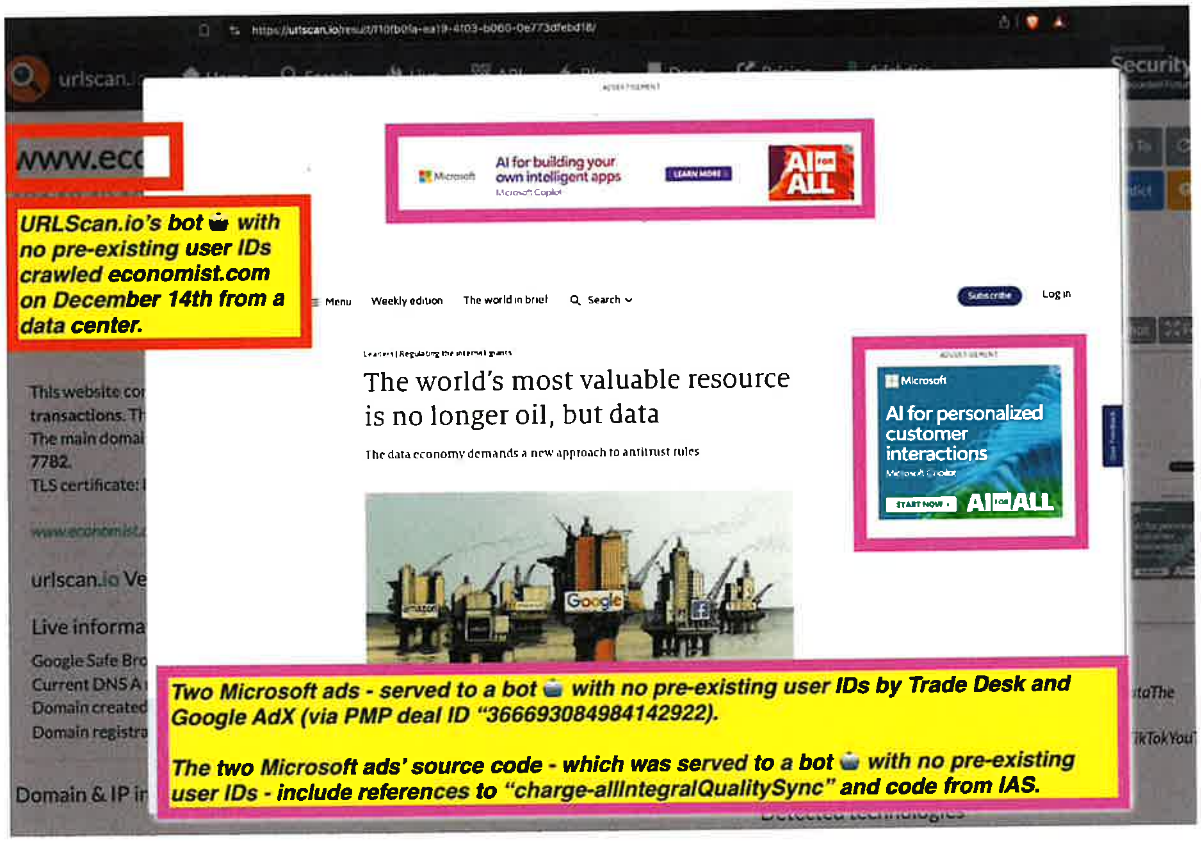
Muted, auto-playing, outstream Hersheys Rolo candy video ad - which may have been intended for a consumer in the USA 🇺🇸 - served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Kargo, both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Charleston, West Virginia 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

The Hersheys ad source code - which was served to a bot 🤖 - included references to "charge-allIntegralQualitySync" and code from IAS.

A Hershey's Rolo candy video ad that was served to URLScan.io's bot. The source code of the Hershey's ad appears to contain references to "charge-allIntegralQualitySync". Source: https://urlscan.io/result/84886d76-1699-4d22-a0f9-e4a7d6f53bcf/#summary

As another example, two ads for Microsoft Copilot AI were served to URLScan.io's bot whilst the bot was crawling economist.com from a data center on December 14th, 2024. The Microsoft ads appear to include references to “charge-allIntegralQualitySync” and code from IAS.



URLScan.io’s bot with no pre-existing user IDs crawled economist.com on December 14th from a data center.

The world’s most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules

Two Microsoft ads - served to a bot with no pre-existing user IDs by Trade Desk and Google AdX (via PMP deal ID “366693084984142922).

The two Microsoft ads’ source code - which was served to a bot with no pre-existing user IDs - include references to “charge-allIntegralQualitySync” and code from IAS.

https://urlscan.io/result/f10fb0fa-ea19-4f03-b060-0e773dfebd18/
urlscan.io
www.eco
Microsoft
AI for building your own intelligent apps
Microsoft Copilot
LEARN MORE
AI FOR ALL
Menu
Weekly edition
The world in brief
Search
Subscribe
Log in
Leaders | Regulating the internet giants
Microsoft
AI for personalized customer interactions
Microsoft Copilot
START NOW
AI FOR ALL
Google

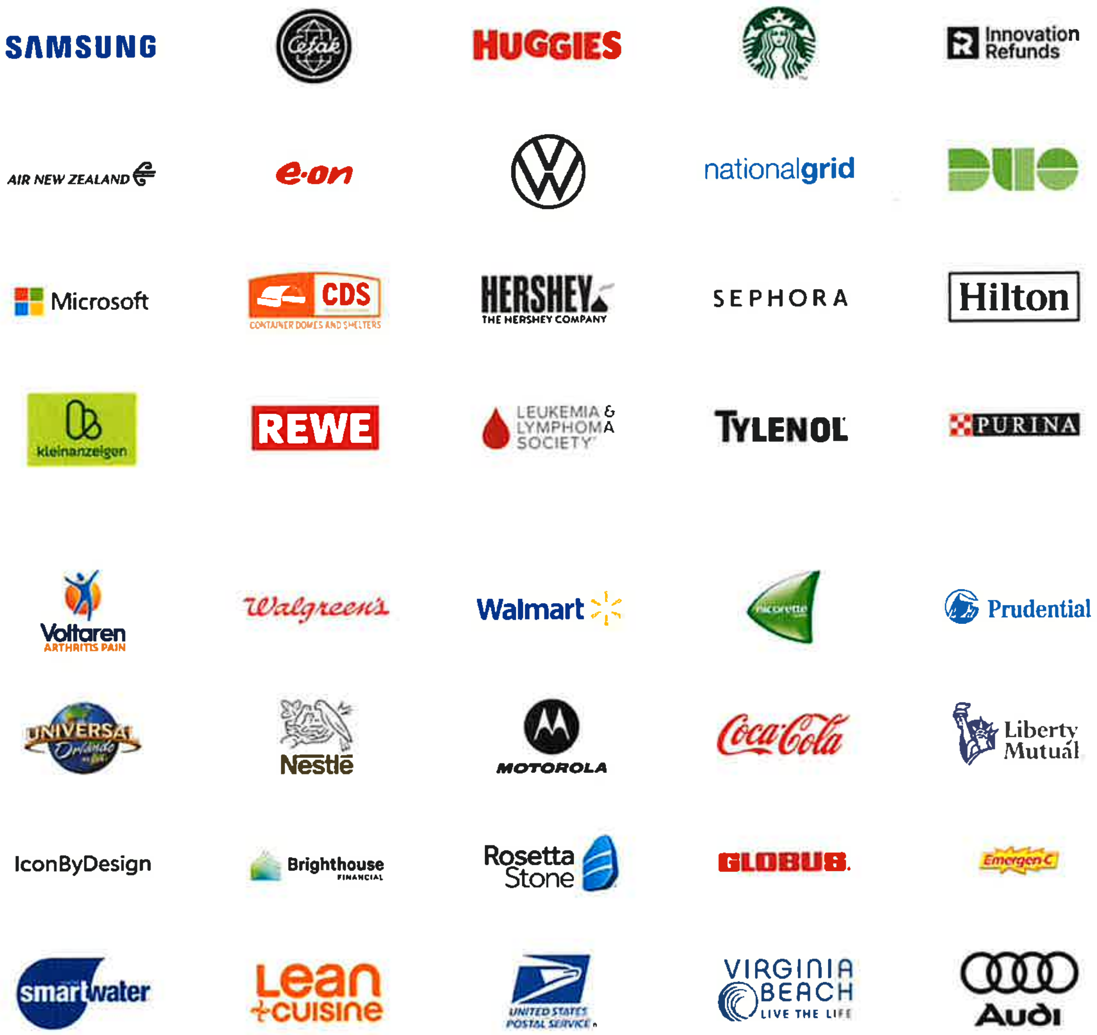
Screenshot of two Microsoft ads served to URLScan.io’s bot. The source code of the Microsoft ads includes references to “charge-allIntegralQualitySync” and code from IAS.

Source: https://urlscan.io/result/f10fb0fa-ea19-4f03-b060-0e773dfebd18/#summary

A sample list of the brands whose ads were served to URLScan.io’s bots and whose ads included references to “charge-allIntegralSuspiciousActivity” or “charge-allIntegralQualitySync” is shown below.

https://adalytics.io/blog/prebid-bot-filtration

Brands whose ads referenced "charge-allIntegralQualitySync" or "charge-allIntegralSuspiciousActivity" & were served to URLScan.io bots



On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

Mobil
adtaxi
ADF CAREERS
Room&Board
Prodly
Harley-Davidson
McCormick
Leafguard
Modibodi
Jet2
TRELEGY ELLIPTA
Neutrogena
NEW ORLEANS
OPRY
POINTSBET SPORTSBOOK • CASINO
JPMORGAN CHASE & CO.
bv Brandywine Valley

Research Results: YouTube TrueView ads served to bots on Google Video Partner sites

According to Google's public online documentation, "Google video partners are high-quality publisher websites and mobile apps where you can show your video ads to viewers beyond YouTube." "Video partner publishers are carefully vetted and must meet Google's inventory quality standards. Video partner publishers also need to follow the policies applicable to their ad management platform (which can include Google Ad Manager, AdMob, or AdSense). Our Video Ad Safety Promise, in which certain types of content can't be monetized for ads, applies to both YouTube and Google video partners."

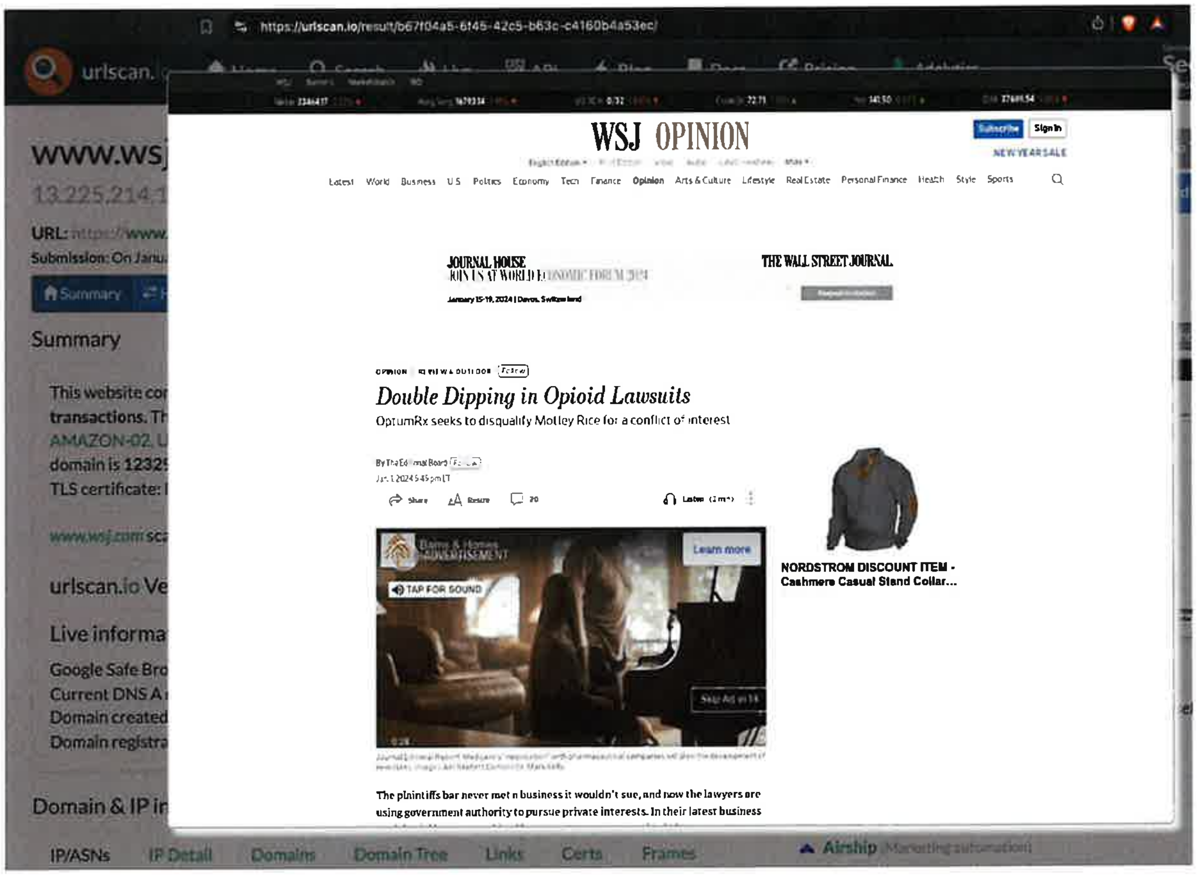
TrueView was Google's "proprietary cost-per-view, choice-based ad format that serves on YouTube, millions of apps, and across the web." With TrueView, advertisers only pay "for actual views of their ads, rather than impressions." TrueView asks users if they want to skip the video ad after 5 seconds with a visual prompt. Google's policies stated that TrueView ads must be skippable, audible, and playing of the video (and ad) cannot be solely initiated by passive user scrolling.

According to another piece of Google's documentation on "Outstream video ad[s]", outstream video ads " serve on partner sites and apps outside of YouTube", and "the ads start with the sound off and the user can tap the ad to unmute it."

One can observe many instances where TrueView video ads from various advertisers were served to bots rather than humans, including in environments where those ads were served entirely muted (with sound off) and without the user clicking on the video to initiate media playback.

For example, January 2nd, 2024 one can see that a TrueView video ad for the Timberlyne Group was served to a bot operating out of a datacenter in a muted, auto-playing video player. The video ad was served to a bot that was crawling wsj.com.The video ad is fully muted and autoplays without user initiation, when served to the bot.

The IP address where the bot was operating out of IP address 185.172.52.56, when served the Timberlyne video ad and this IP address is owned by PacketHub S.A. and is hosted in St Louis, US. This IP belongs to datacenter infrastructure.



Double Dipping in Opioid Lawsuits

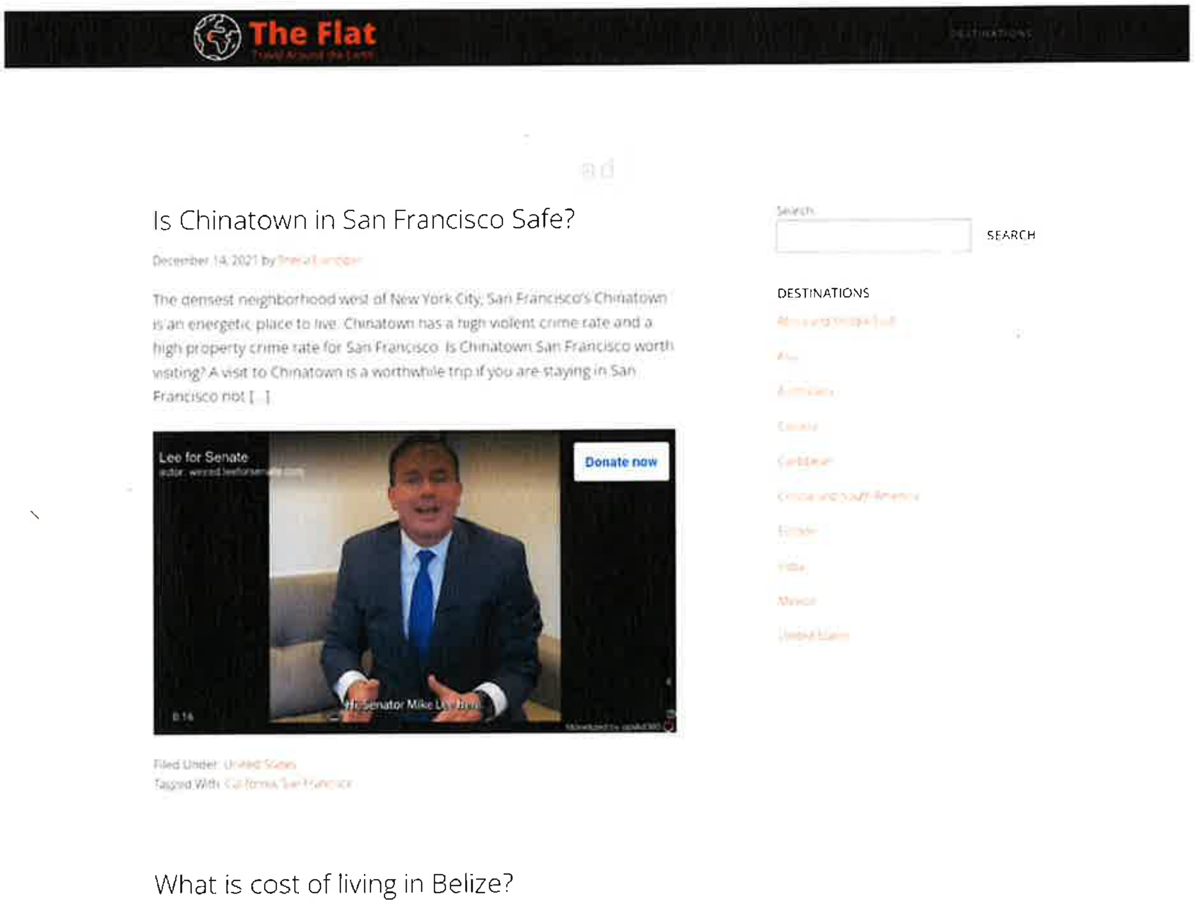
OptumRx seeks to disqualify Motley Rice for a conflict of interest

The plaintiffs bar never met a business it wouldn't sue, and now the lawyers are using government authority to pursue private interests. In their latest business

Screenshot of a Timberlyne Group YouTube TrueView video ad served to a bot in a datacenter on a muted, auto-playing video player on January

2nd, 2024. Source: https://urlscan.io/result/b67f04a5-6f45-42c5-b63c-c4160b4a53ec/

As another example, on October 25th, 2022, one can see that a TrueView video ad for the Mike Lee for Senate was served to a bot operating out of a datacenter in a muted, auto-playing video player. The video ad was served to a bot that was crawling theflatbkny.com.The video ad is fully muted and autoplays without user initiation, when served to the bot.



Is Chinatown in San Francisco Safe?

December 14, 2021 by [illegible]

The densest neighborhood west of New York City, San Francisco's Chinatown is an energetic place to live. Chinatown has a high violent crime rate and a high property crime rate for San Francisco. Is Chinatown San Francisco worth visiting? A visit to Chinatown is a worthwhile trip if you are staying in San Francisco not [...]

Filed Under: United States
Tagged With: California, San Francisco

Search
SEARCH

DESTINATIONS

Africa and Middle East
Asia
Australia
Canada
Caribbean
Central and South America
Europe
India
Mexico
United States

What is cost of living in Belize?

Screenshot of a Sen. Mike Lee for Senate YouTube TrueView video ad served to a bot in a datacenter on a muted, auto-playing video player on October 25th, 2022. Source: https://urlscan.io/result/7f159e54-302f-4da6-9f67-e9313eef2fe4/

Research Results: Google's publisher ad server appears to have served millions of impressions from

thousands of advertisers to bots, including declared bots operating out of Google's own data centers

Many of the websites observed serving ads to bots for years appear to be utilizing Google Ad Manager (GAM) as their publisher ad server. This can be deduced by the presence of specific HTTPS requests and by the presence of Google Publisher Tag on their pages. The Google Publisher Tag (GPT) is an ad tagging library for Google Ad Manager. A future report will analyze the prevalence of ads being served by Google Ad Manager to declared bots in known data centers.

According to Check My Ads Institute (CMAI), which observed the United States vs. Google LLC trial proceedings in September, 2024, Per Bjorke (Director of Product Management, AdSpam Team at Google) commented under oath about Google's bot and invalid traffic filtration systems.

According to Check My Ads' recounting:

"[Bjorke] talks about all Google does to combat Invalid Traffic and ad fraud, and Google's ~$250M investment in the area in '22. He explains how IVT matters to advertisers, as they wouldn't want to pay for traffic from bots sitting in a data center somewhere. He speaks to the publisher vetting process, and how keeping bad actors out of the AdX system is important, so Google doesn't need to battle them later on. We hear about how they have a refund and claw-back process to make sure advertisers don't pay for and publishers aren't paid for IVT. Google points to AWbid to try to show how fraud and spam was more prevalent on third party exchanges, and Bjorke explains why it is much easier to contain in a closed system."

Research Results: Hundreds of thousands of United States government healthcare.gov ads were served to bots operating out of Google's own data centers

Hundreds of thousands of healthcare.gov ads (Department of Health and Human Services) appear to have been served for years to declared bots operating out of Google Cloud data center IP addresses. Specifically. healthcare.gov ads were served to the HTTP Archive bot from 2022 to

2024. The bot is a declared bot, whose user agent is on the IAB Bots and Spiders List.

For example, the following healthcare.gov ad creative was served at least 41,141 times to the declared HTTP Archive bot:

LOST
IOWA
MEDICAID
HealthCare.gov
is here for you
ENROLL TODAY!

Source: https://s0.2mdn.net/simgad/9542029637209407237

A similar healthcare.gov ad was served 33,107 times to HTTP Archive's bot between 2022 and 2024.

LOST
UTAH
MEDICAID
HealthCare.gov
is here for you
ENROLL TODAY!

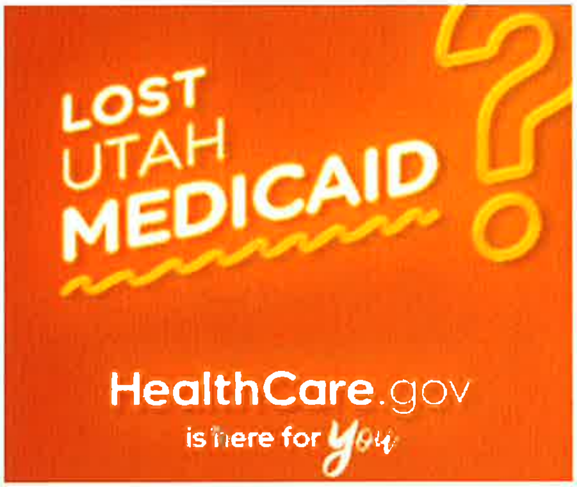
Source: https://s0.2mdn.net/simgad/8208861446627735063

The following healthcare.gov ad was served 28,702 times to HTTP Archive's declared bot operating out of a Google Cloud data center.

LOST
IOWA
MEDICAID
HealthCare.gov
is here for you

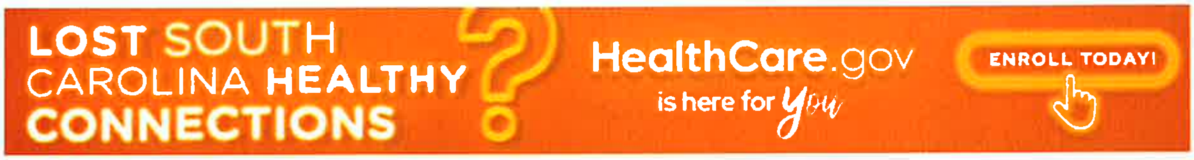
Source: https://s0.2mdn.net/simgad/10082509476545170 80

The following healthcare.gov ad was served 23,479 times to HTTP Archive's declared bot operating out of a Google Cloud data center.



Source: https://s0.2mdn.net/simgad/15936844823979823746

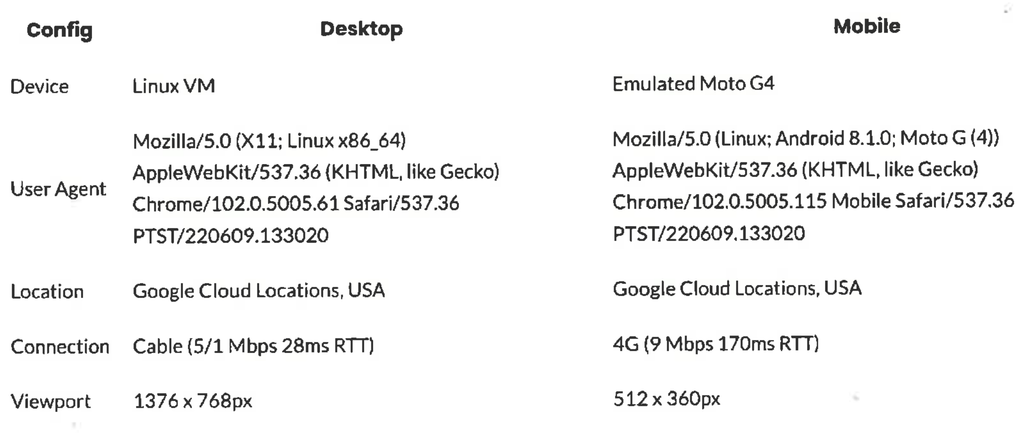
The following healthcare.gov ad was served 12,550 times to HTTP Archive's declared bot operating out of a Google Cloud data center IP address.



Source: https://s0.2mdn.net/simgad/8871931525062578142

Research Results: Publishers who were seen consistently NOT serving ads to HTTP Archive's declared bot

As described in the methodology section towards the beginning of this research report, this study sourced data from several distinct bot and crawler datasets. One of those datasets was the HTTP Archive, which utilizes a declared bot operating out of Google Cloud data center IP addresses to crawl several million websites each month. The HTTP Archive bot's bot is a declared bot - because it specifically communicates its status as a bot via the User-Agent header.



Config	Desktop	Mobile
Device	Linux VM	Emulated Moto G4
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020	Mozilla/5.0 (Linux; Android 8.1.0; Moto G (4)) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.115 Mobile Safari/537.36 PTST/220609.133020
Location	Google Cloud Locations, USA	Google Cloud Locations, USA
Connection	Cable (5/1 Mbps 28ms RTT)	4G (9 Mbps 170ms RTT)
Viewport	1376 x 768px	512 x 360px

Screenshot from HTTP Archive's public documentation page, showing the exact declared bot user agent used by the bot. Source: https://almanac.httparchive.org/en/2022/methodology

The User-Agent header is an HTTP header intended to identify the user agent responsible for making a given HTTP request. When a person browses the web via a browser on their phone rather than on the desktop, their phone's browser declares via the HTTP header that the user is browsing the web on a mobile browser (rather than a desktop browser).

Similarly, when various "good" bots, such as GoogleBot or BingBot crawl the open internet, those bots openly declare themselves via the HTTP User-Agent header. If a website does not want to appear in Google or Bing search results, they can choose to block GoogleBot or Bingbot via their web hosting provider.

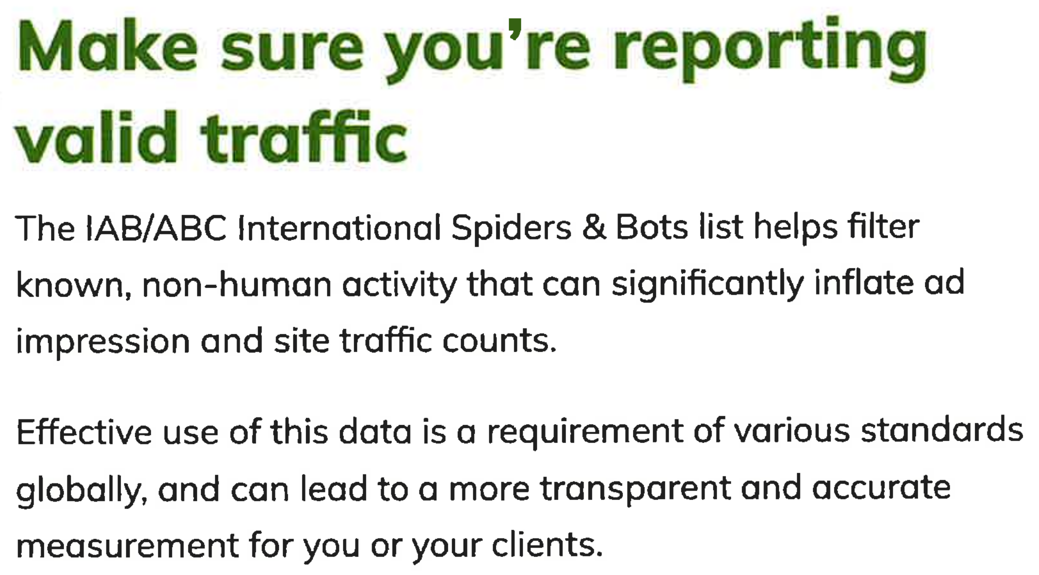
The HTTP Archive bot's user agent has been on the IAB Tech Lab's Bots and Spiders reference list since 2013.

According to the IAB Tech Lab, "The IAB Tech Lab publishes a comprehensive list of such Spiders and Robots that helps companies identify automated traffic such as search engine crawlers, monitoring tools, and other non-human traffic that they don't want included in their analytics and billable counts [...] The IAB Tech Lab Spiders and Robots provides the industry two main purposes. First, the spiders and robots list consists of two text files: one for valid browsers or user agents and one for known robots. These lists are intended to be used together to comply with the “dual pass” approach to filtering as defined in the IAB’s Ad Impression Measurement Guidelines (i.e., identify valid transactions using the valid browser list and then filter/remove invalid transactions using the known robots list). Second, the spiders and robots list supports the MRC’s General Invalid Traffic Detection and Filtration Standard by providing a common industry resource and list for facilitating IVT detection and filtration.”

According to IAB Europe, “Traffic consisting of robotic user agents is non-human rather than fraudulent; the technology exists to be helpful to internet users and has not been ‘disguised’ as a human user. This means that they can be **easily detected and filtered by implementing the Spiders & Robots list**” (emphasis added).

Source: https://iabeurope.eu/international-iababc-spiders-and-bots-list/

According to the Audit Bureau of Circulations (ABC UK), “*The IAB/ABC International Spiders & Bots list helps filter known, non-human activity that can significantly inflate ad impression and site traffic counts. Effective use of this data is a requirement of various standards globally, and can lead to a more transparent and accurate measurement for you or your clients.*”



Make sure you're reporting valid traffic

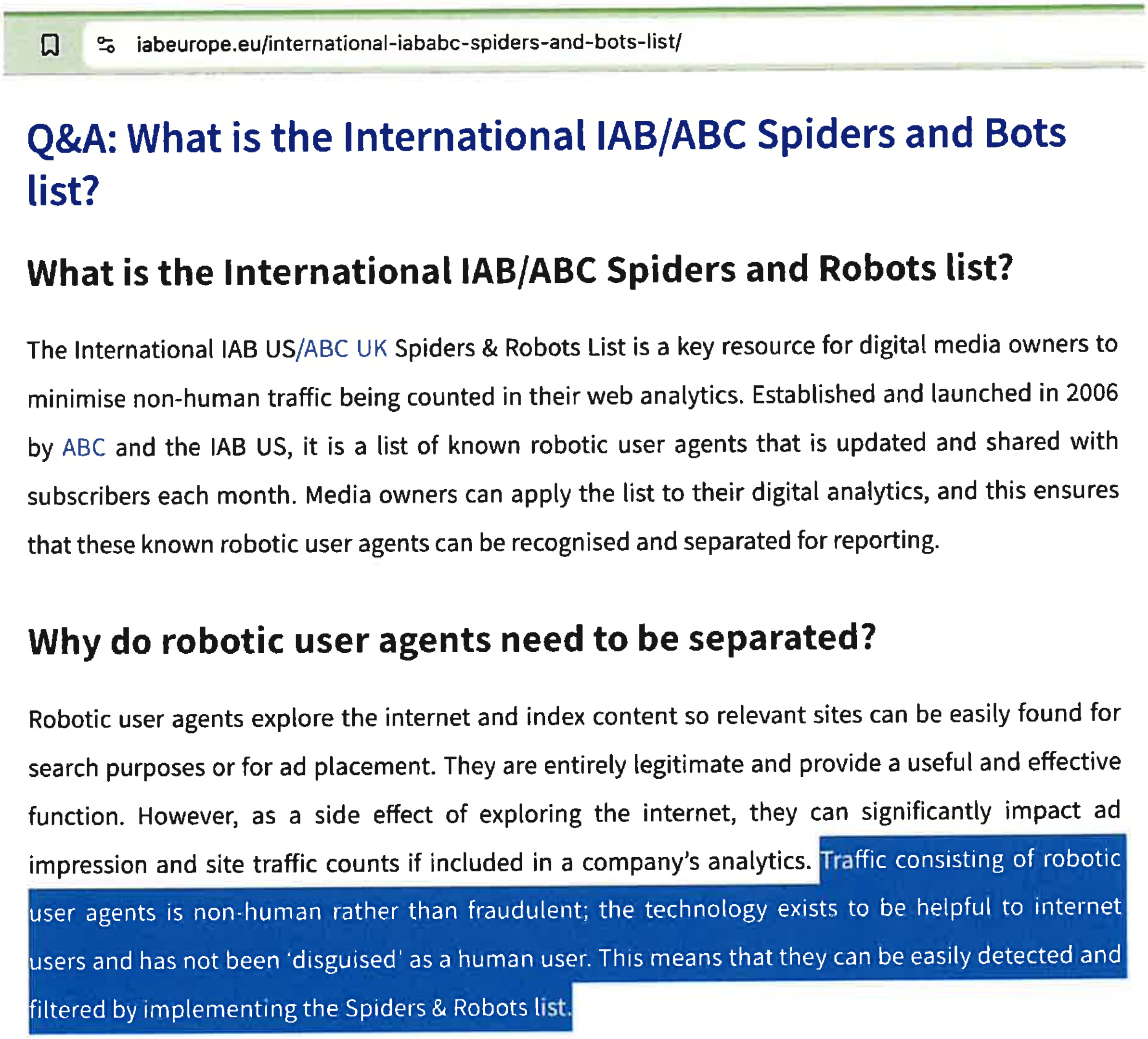
The IAB/ABC International Spiders & Bots list helps filter known, non-human activity that can significantly inflate ad impression and site traffic counts.

Effective use of this data is a requirement of various standards globally, and can lead to a more transparent and accurate measurement for you or your clients.

Source: https://www.abc.org.uk/assurance/bots-and-spiders

As previously documented, this study observed many instances where ad tech vendors appeared to serve ads to declared bots whose user agent is on the IAB Tech Lab's Bots list.

Similarly, many different digital publishers and websites were observed serving digital ads to



Q&A: What is the International IAB/ABC Spiders and Bots list?

What is the International IAB/ABC Spiders and Robots list?

The International IAB US/ABC UK Spiders & Robots List is a key resource for digital media owners to minimise non-human traffic being counted in their web analytics. Established and launched in 2006 by ABC and the IAB US, it is a list of known robotic user agents that is updated and shared with subscribers each month. Media owners can apply the list to their digital analytics, and this ensures that these known robotic user agents can be recognised and separated for reporting.

Why do robotic user agents need to be separated?

Robotic user agents explore the internet and index content so relevant sites can be easily found for search purposes or for ad placement. They are entirely legitimate and provide a useful and effective function. However, as a side effect of exploring the internet, they can significantly impact ad impression and site traffic counts if included in a company's analytics. Traffic consisting of robotic user agents is non-human rather than fraudulent; the technology exists to be helpful to internet users and has not been 'disguised' as a human user. This means that they can be easily detected and filtered by implementing the Spiders & Robots list.

declared bots on IAB Tech Lab's bots list. This includes many publishers who appear to utilize IAS and DoubleVerify's pre-bid publisher optimization tools on their pages, such as washingtonpost.com, usatoday.com, weather.com, cnn.com, fandom.com, and wired.com.

For example, nytimes.com was observed serving ads for Jaeger-LeCoultre whilst the declared HTTP Archive bot was crawling the website in May 2022.

Weather.com - which currently appears to use DoubleVerify's publisher optimization tool and previously appeared to use IAS's publisher optimization tool - was observed serving ads for Samsung, Haleon Flonase, Togo's restaurants, Brighthouse Financial, Unilever Murad, American Airlines, Procter & Gamble Bounty Towels, DC Water, and Progressive insurance whilst the HTTP Archive bot was crawling the website in 2022, 2023, and/or 2024.

Usatoday.com - which appears to use IAS' publisher optimization tool on its webpages - was observed serving ads for JPMorgan Chase, T-Mobile, the Government of Utah, and Bank of America to the HTTP Archive bot whilst the bot was crawling the website in 2022, 2023, and/or 2024.

Warner Bros. Discovery operated CNN.com - which appears to use IAS' publisher optimization tool on its webpages - was observed serving ads for Jaeger-LeCoultre and Vista Paint to the HTTP Archive bot whilst the bot was crawling the website in 2022.

Conde Nast operated Wired.com - which appears to use IAS' publisher optimization tool on its webpages - was observed serving ads for T-Mobile to the HTTP Archive bot whilst the bot was crawling the website in February 2022.

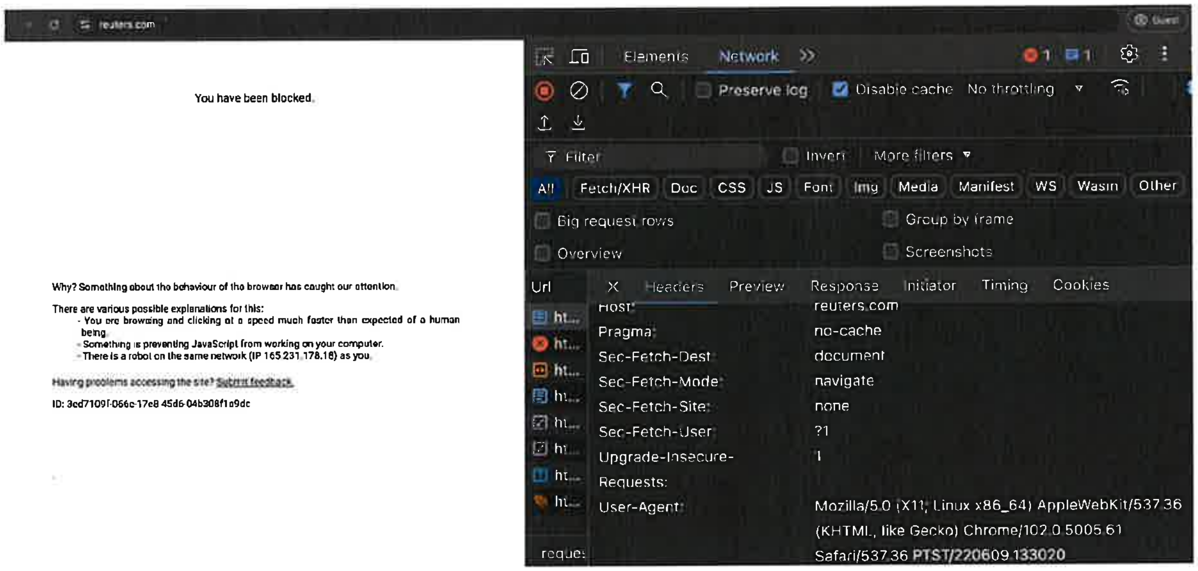
Fandom.com - which appears to use both IAS' and DoubleVerify’s publisher optimization tool on its webpages - was observed serving ads for T-Mobile, US Bank, Progressive, Apple, and the Virginia College Savings Plan (Virginia529) to the HTTP Archive bot whilst the bot crawling the website in 2022-2024.

However, analyzing years of HTTP Archive data reveals a notable “absence” of ad delivery to the declared HTTP Archive bot on a few websites. For example, there are a few websites that have been regularly crawled by the HTTP Archive bot, yet for which there appears to be no records of ads being served to that bot on those specific pages.

One can use a standard chrome browser and chrome developer tools’ Network conditions setting or a custom browser extension to modify the declared browser user agent declared by the browser. For example, if a consumer is using Chrome on Windows, one can use a browser extension to make it appear as though the device is GoogleBot, BingBot, or another type of crawler. With this capability, one can emulate the exact user agent used by HTTP Archive’s bot when it is crawling the web.

Emulating the HTTP Archive declared bot user agent via Chrome developer tools shows that some websites consistently and completely block any ads from being served to a user declaring themselves to be a bot.

For example, in the screenshot below, one can see that if a user declares themselves to be the user agent that is used by HTTP Archive bot, Reuters' website blocks the user and does not show any ads whatsoever.



You have been blocked.

Why? Something about the behaviour of the browser has caught our attention.

There are various possible explanations for this:

- You are browsing and clicking at a speed much faster than expected of a human being.
- Something is preventing JavaScript from working on your computer.
- There is a robot on the same network (IP 165.231.178.18) as you.

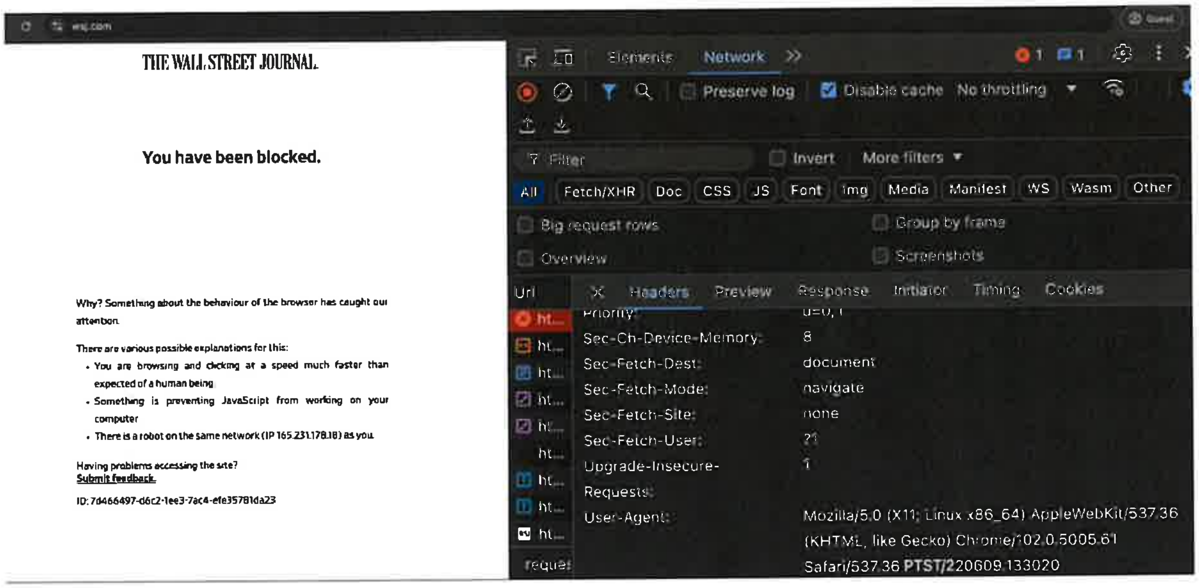
Having problems accessing the site? Submit feedback.

ID: 3cd7109f-066c-17e8 45d6-04b308f1a9dc

Host: reuters.com
Pragma: no-cache
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020

Reuters.com blocks the user if the user is a declared bot.

Similarly, the website of the Wall Street Journal wsj.com also blocks the user if the user declares themself to be a bot via the HTTP User-Agent request header.



THE WALL STREET JOURNAL.

You have been blocked.

Why? Something about the behaviour of the browser has caught our attention.

There are various possible explanations for this:

- You are browsing and clicking at a speed much faster than expected of a human being
- Something is preventing JavaScript from working on your computer
- There is a robot on the same network (IP 165.231.178.18) as you.

Having problems accessing the site?
Submit feedback.

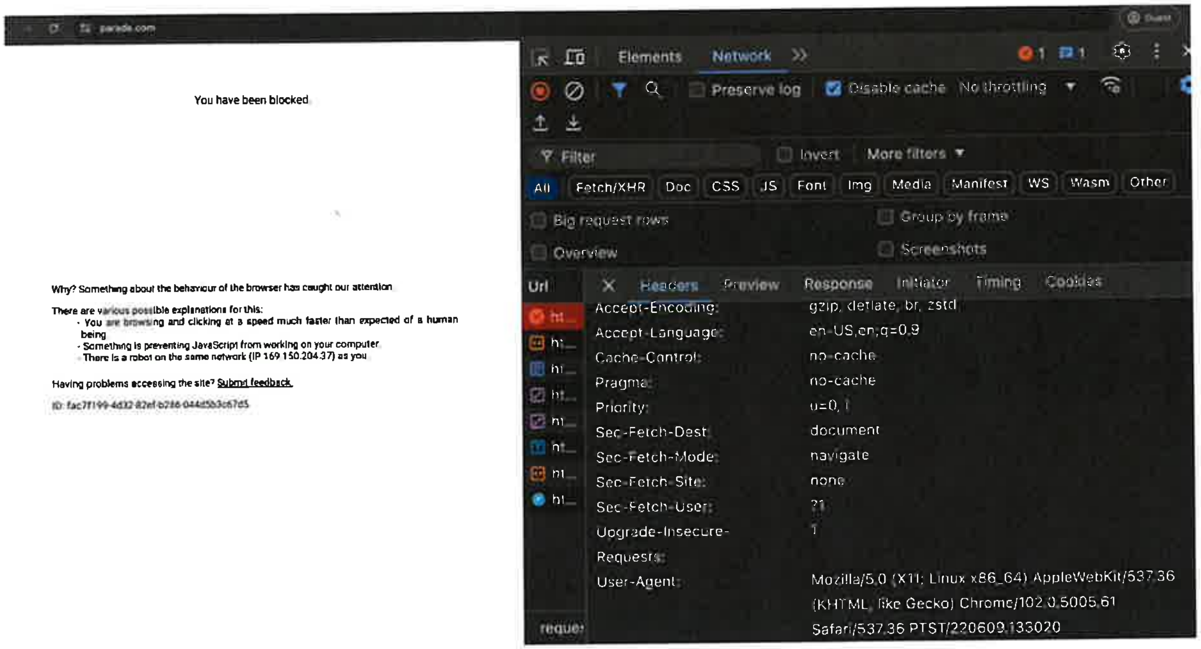
ID: 7d466497-d6c2-1ee3-7ac4-efe35781da23

```
Priority:                     u=0, i
Sec-Ch-Device-Memory:         8
Sec-Fetch-Dest:               document
Sec-Fetch-Mode:               navigate
Sec-Fetch-Site:               none
Sec-Fetch-User:               ?1
Upgrade-Insecure-             1
Requests:
User-Agent:                   Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                              (KHTML, like Gecko) Chrome/102.0.5005.61
                              Safari/537.36 PTST/220609.133020
```

The Wall Street Journal's website wsj.com blocks the user if the user is a declared bot.

Many websites owned or operated by a media company called the Arena Group also appear to block users who declare themselves to be a bot via the HTTP User Agent request header. For example, in the screenshots below, one can see how the websites parade.com, autoblog.com, pethelpful.com, athlonsports.com, thestreet.com, mensjournal.com, and surfer.com all appear to block the user and do not serve any ads if the user is a declared bot like the HTTP Archive bot.

https://adalytics.io/blog/prebid-bot-filtration



You have been blocked

Why? Something about the behaviour of the browser has caught our attention

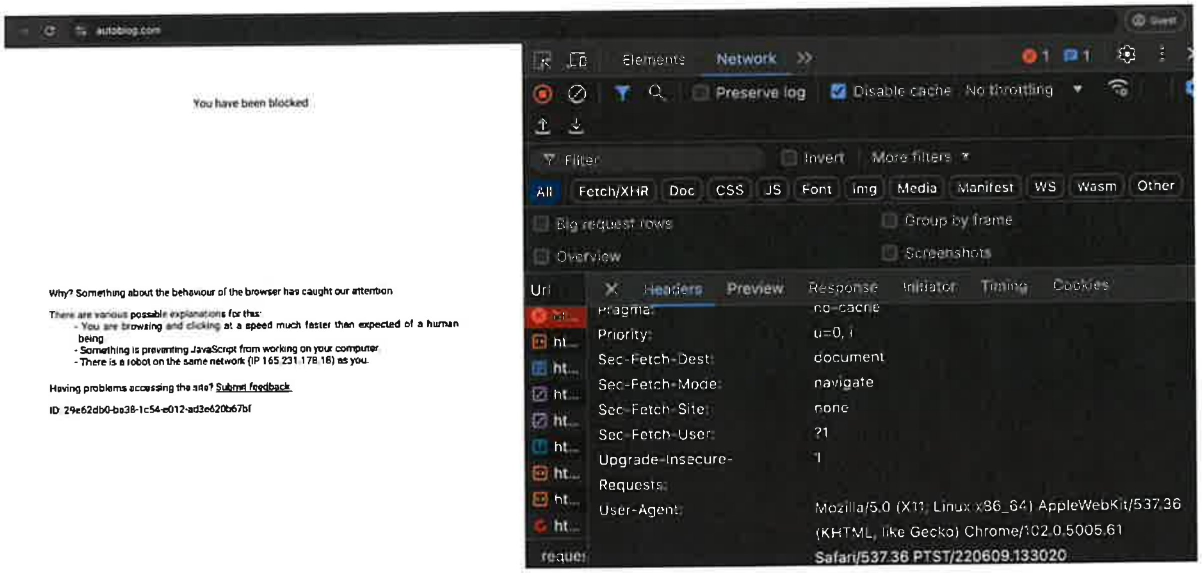
There are various possible explanations for this:
- You are browsing and clicking at a speed much faster than expected of a human being
- Something is preventing JavaScript from working on your computer
- There is a robot on the same network (IP 169 150.204.37) as you

Having problems accessing the site? Submit feedback.

ID: fac7f199-4d32-82ef-b286-044d5b3c67d5

```
Accept-Encoding:            gzip, deflate, br, zstd
Accept-Language:            en-US,en;q=0.9
Cache-Control:              no-cache
Pragma:                     no-cache
Priority:                   u=0, i
Sec-Fetch-Dest:             document
Sec-Fetch-Mode:             navigate
Sec-Fetch-Site:             none
Sec-Fetch-User:             ?1
Upgrade-Insecure-           1
Requests:
User-Agent:                 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                            (KHTML, like Gecko) Chrome/102.0.5005.61
                            Safari/537.36 PTST/220609.133020
```

Arena Group managed parade.com blocks the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.



You have been blocked

Why? Something about the behaviour of the browser has caught our attention

There are various possible explanations for this:
- You are browsing and clicking at a speed much faster than expected of a human being
- Something is preventing JavaScript from working on your computer
- There is a robot on the same network (IP 165.231.178.18) as you.

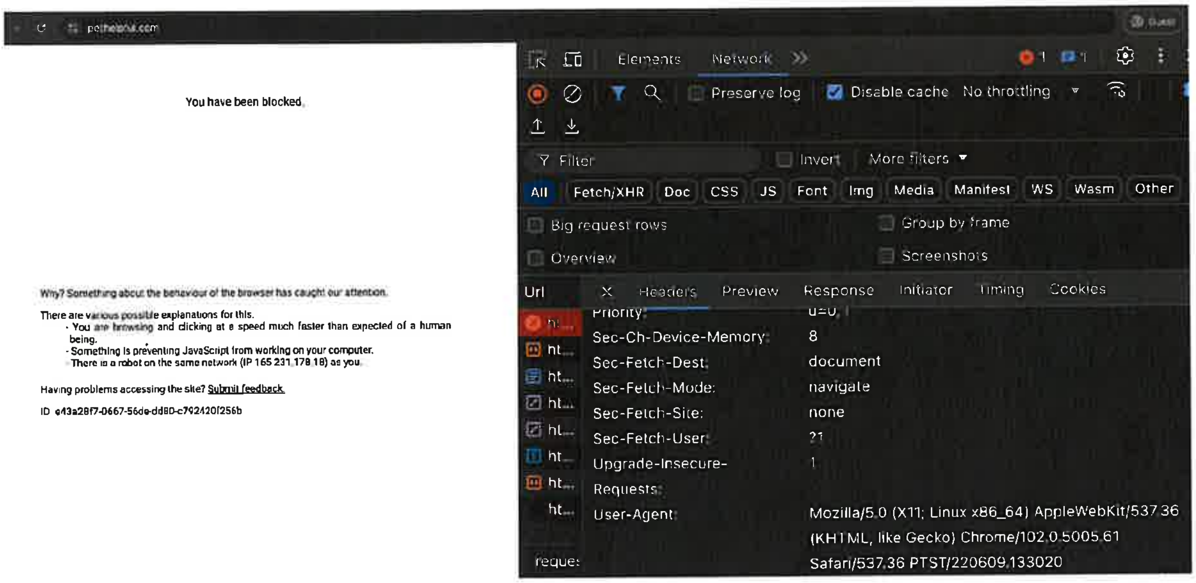
Having problems accessing the site? Submit feedback.

ID: 29e62db0-ba38-1c54-e012-ad3e620b67bf

```
Pragma:                     no-cache
Priority:                   u=0, i
Sec-Fetch-Dest:             document
Sec-Fetch-Mode:             navigate
Sec-Fetch-Site:             none
Sec-Fetch-User:             ?1
Upgrade-Insecure-           1
Requests:
User-Agent:                 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                            (KHTML, like Gecko) Chrome/102.0.5005.61
                            Safari/537.36 PTST/220609.133020
```

Arena Group managed autoblog.com blocks the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.

https://adalytics.io/blog/prebid-bot-filtration



You have been blocked.

Why? Something about the behaviour of the browser has caught our attention.

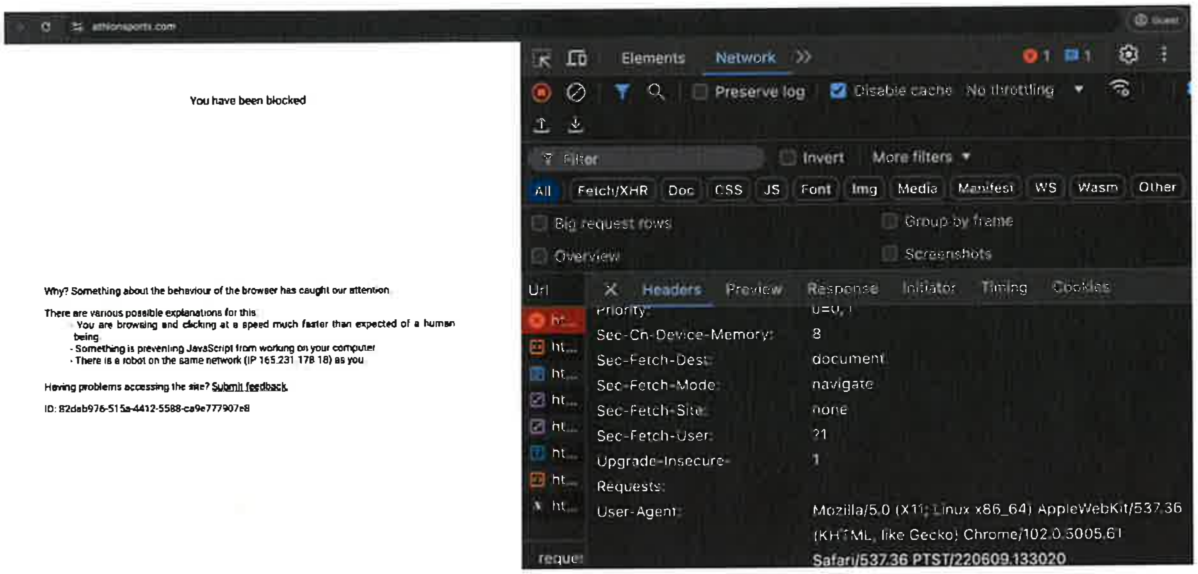
There are various possible explanations for this.
- You are browsing and clicking at a speed much faster than expected of a human being.
- Something is preventing JavaScript from working on your computer.
- There is a robot on the same network (IP 165.231.178.18) as you.

Having problems accessing the site? Submit feedback.

ID e43a28f7-0667-56de-dd80-c792420f256b

```
Priority:                    u=0, i
Sec-Ch-Device-Memory:        8
Sec-Fetch-Dest:              document
Sec-Fetch-Mode:              navigate
Sec-Fetch-Site:              none
Sec-Fetch-User:              ?1
Upgrade-Insecure-            1
Requests:
User-Agent:                  Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                             (KHTML, like Gecko) Chrome/102.0.5005.61
                             Safari/537.36 PTST/220609.133020
```

Arena Group managed pethelpful.com blocks the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.



You have been blocked

Why? Something about the behaviour of the browser has caught our attention

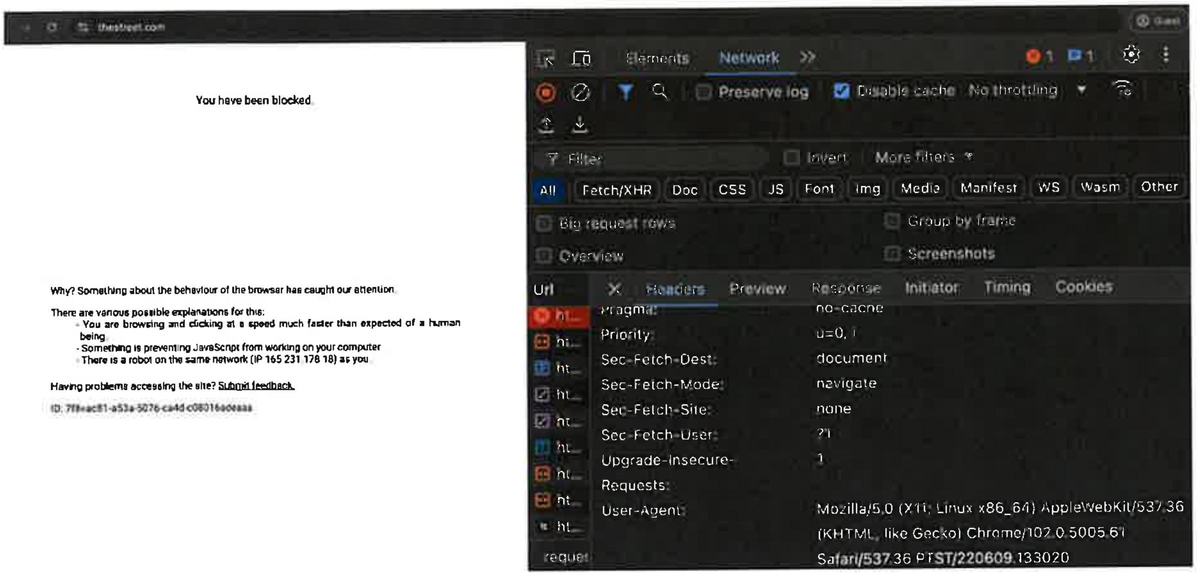
There are various possible explanations for this
- You are browsing and clicking at a speed much faster than expected of a human being
- Something is preventing JavaScript from working on your computer
- There is a robot on the same network (IP 165.231.178.18) as you

Having problems accessing the site? Submit feedback.

ID: 82dab976-515a-4412-5588-ca9e777907e8

```
Priority:                    u=0, i
Sec-Ch-Device-Memory:        8
Sec-Fetch-Dest:              document
Sec-Fetch-Mode:              navigate
Sec-Fetch-Site:              none
Sec-Fetch-User:              ?1
Upgrade-Insecure-            1
Requests:
User-Agent:                  Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                             (KHTML, like Gecko) Chrome/102.0.5005.61
                             Safari/537.36 PTST/220609.133020
```

Arena Group owned athlonsports.com blocks the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.



You have been blocked

Why? Something about the behaviour of the browser has caught our attention.

There are various possible explanations for this:

- You are browsing and clicking at a speed much faster than expected of a human being
- Something is preventing JavaScript from working on your computer
- There is a robot on the same network (IP 165 231 178 18) as you

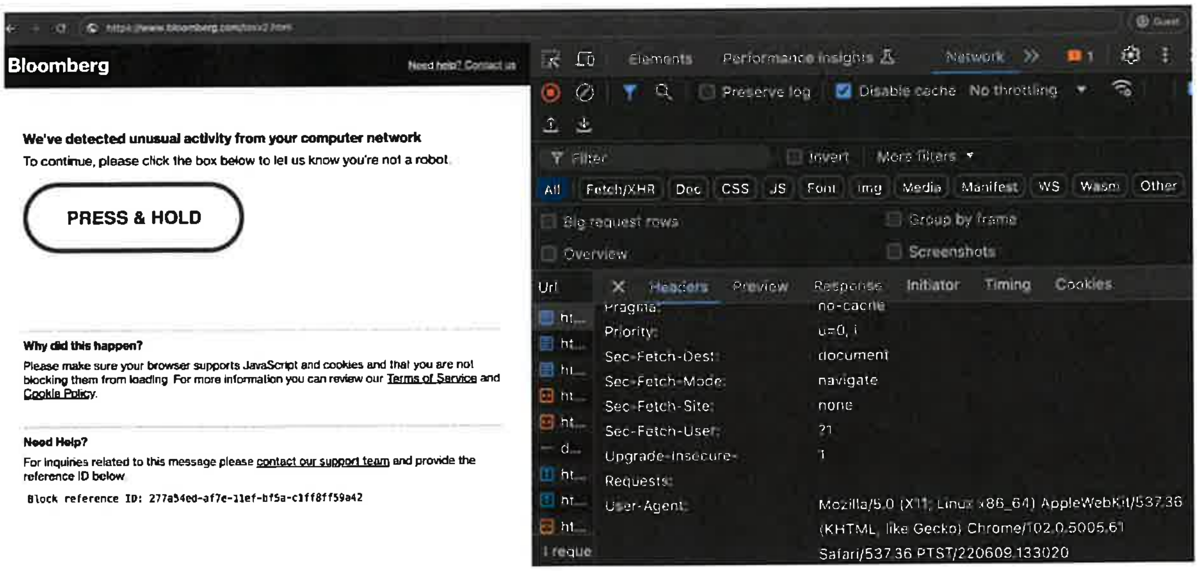
Having problems accessing the site? Submit feedback.

ID: 7f8eac81-a53a-5076-ca4d-c08016adeaaa

```
Pragma:                     no-cache
Priority:                   u=0, i
Sec-Fetch-Dest:             document
Sec-Fetch-Mode:             navigate
Sec-Fetch-Site:             none
Sec-Fetch-User:             ?1
Upgrade-Insecure-           1
Requests:
User-Agent:                 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                            (KHTML, like Gecko) Chrome/102.0.5005.61
                            Safari/537.36 PTST/220609.133020
```

Arena Group managed thestreet.com blocks the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.

Bloomberg.com also appears to create a challenge that the user must solve if they declare themselves to be a bot, and do not appear to serve ads initially to the user.



We've detected unusual activity from your computer network

To continue, please click the box below to let us know you're not a robot.

PRESS & HOLD

Why did this happen?

Please make sure your browser supports JavaScript and cookies and that you are not blocking them from loading. For more information you can review our Terms of Service and Cookie Policy.

Need Help?

For inquiries related to this message please contact our support team and provide the reference ID below.

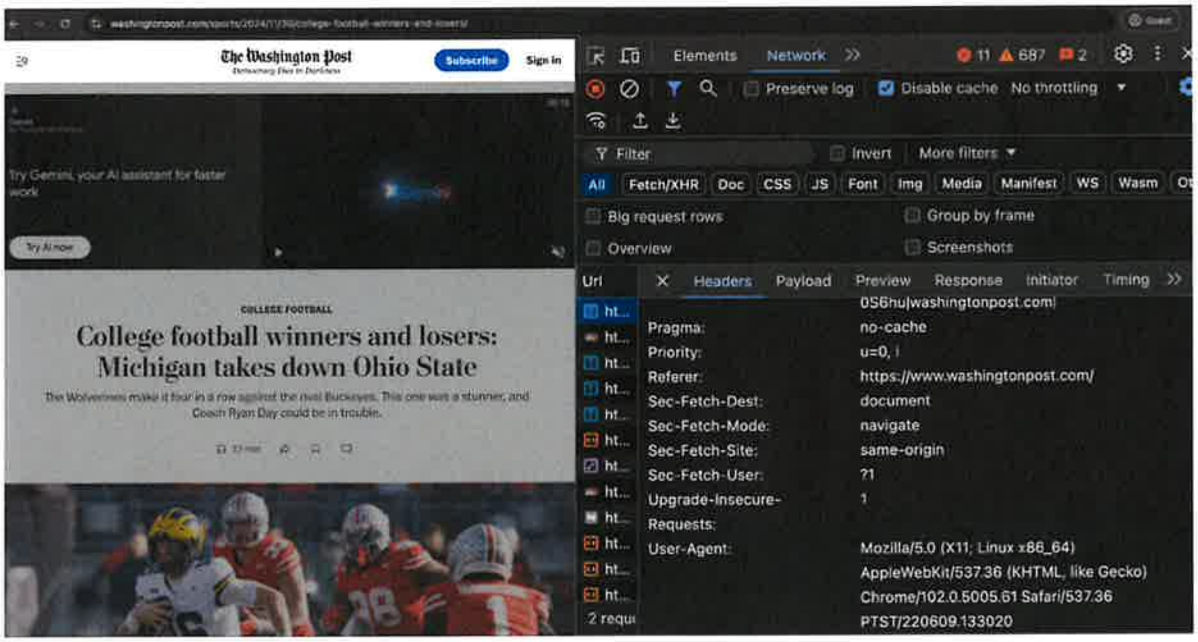
```
Block reference ID: 277a54ed-af7e-11ef-bf5a-c1ff8ff59a42
```

```
Pragma:                     no-cache
Priority:                   u=0, i
Sec-Fetch-Dest:             document
Sec-Fetch-Mode:             navigate
Sec-Fetch-Site:             none
Sec-Fetch-User:             ?1
Upgrade-Insecure-           1
Requests:
User-Agent:                 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
                            (KHTML, like Gecko) Chrome/102.0.5005.61
                            Safari/537.36 PTST/220609.133020
```

Bloomberg.com blocks and challenges the user and does not serve any ads if the user declares themself to be a bot via the HTTP User Agent request header.

One can contrast this difference in behavior by looking at what happens when a user declares themself to be a bot via the HTTP user-agent headers and visits websites such as washingtonpost.com, nytimes.com, weather.com, si.com, cafedlites.com, usatoday.com, weather.com, or fandom.com. As mentioned before, many of these websites were observed serving ads to declared bots such as the HTTP Archive bot.

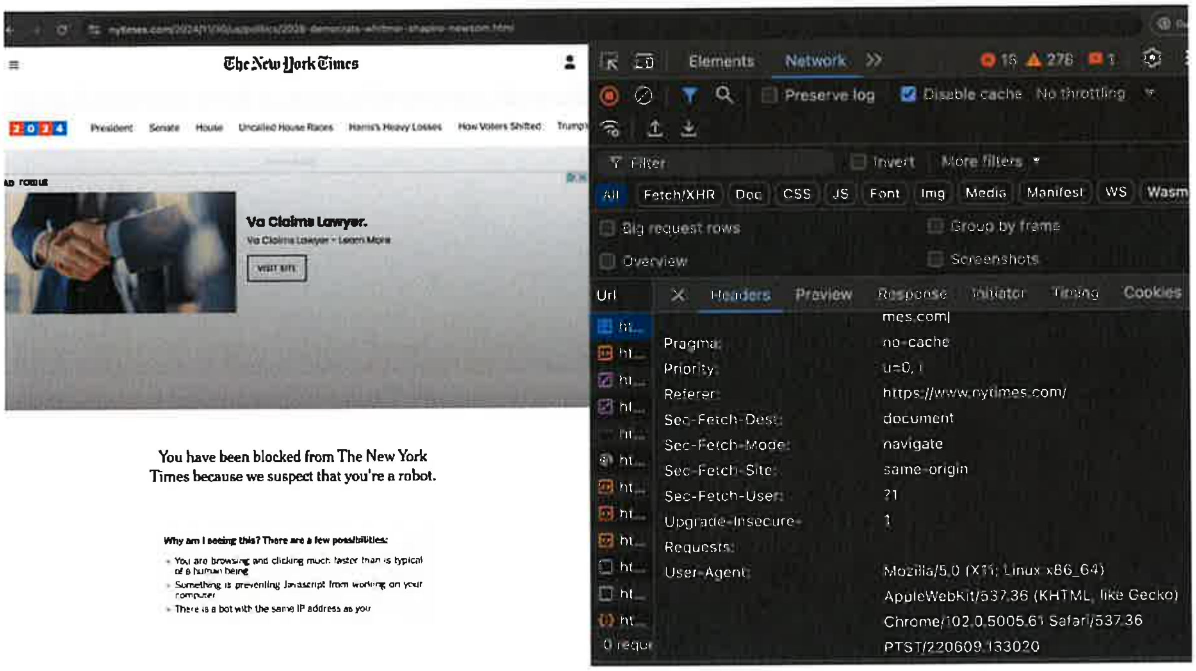
For example, in the screenshot below, one can see that washingtonpost.com serves a Google Gemini AI ad to the user when the user's declared User Agent is a bot on the IAB Tech Labs Bots & Spiders list.



```
                        056hu|washingtonpost.com|
Pragma:                 no-cache
Priority:               u=0, i
Referer:                https://www.washingtonpost.com/
Sec-Fetch-Dest:         document
Sec-Fetch-Mode:         navigate
Sec-Fetch-Site:         same-origin
Sec-Fetch-User:         ?1
Upgrade-Insecure-       1
Requests:
User-Agent:             Mozilla/5.0 (X11; Linux x86_64)
                        AppleWebKit/537.36 (KHTML, like Gecko)
                        Chrome/102.0.5005.61 Safari/537.36
                        PTST/220609.133020
```

washingtonpost.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header.

https://adalytics.io/blog/prebid-bot-filtration



☐ Preserve log ☑ Disable cache No throttling

☐ Big request rows ☐ Group by frame

☐ Overview ☐ Screenshots

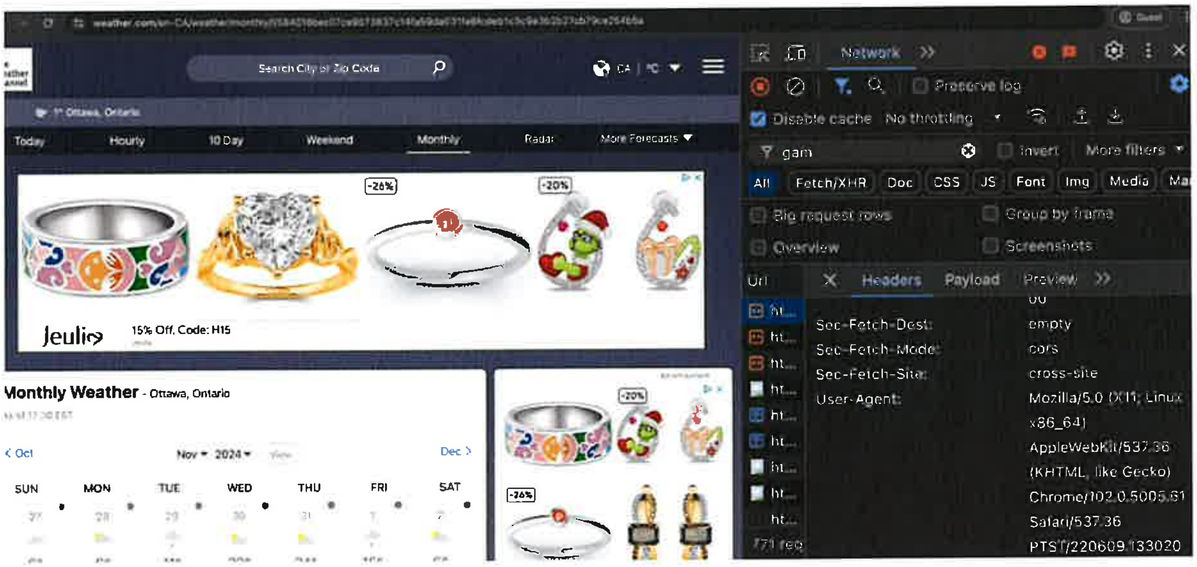
You have been blocked from The New York Times because we suspect that you're a robot.

Why am I seeing this? There are a few possibilities:

- You are browsing and clicking much faster than is typical of a human being
- Something is preventing Javascript from working on your computer
- There is a bot with the same IP address as you

```
                           mes.com|
Pragma:                    no-cache
Priority:                  u=0, i
Referer:                   https://www.nytimes.com/
Sec-Fetch-Dest:            document
Sec-Fetch-Mode:            navigate
Sec-Fetch-Site:            same-origin
Sec-Fetch-User:            ?1
Upgrade-Insecure-          1
Requests:
User-Agent:                Mozilla/5.0 (X11; Linux x86_64)
                           AppleWebKit/537.36 (KHTML, like Gecko)
                           Chrome/102.0.5005.61 Safari/537.36
                           PTST/220609.133020
```

nytimes.com.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header.



☐ Preserve log

☑ Disable cache No throttling

gam

☐ Big request rows ☐ Group by frame

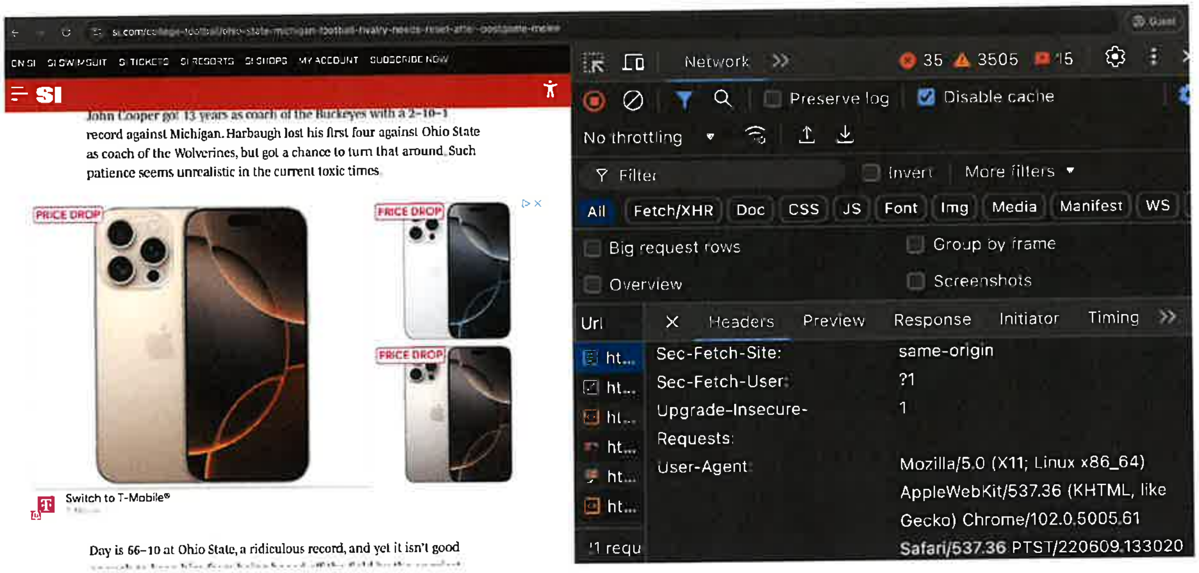
☐ Overview ☐ Screenshots

```
                      00
Sec-Fetch-Dest:       empty
Sec-Fetch-Mode:       cors
Sec-Fetch-Site:       cross-site
User-Agent:           Mozilla/5.0 (X11; Linux
                      x86_64)
                      AppleWebKit/537.36
                      (KHTML, like Gecko)
                      Chrome/102.0.5005.61
                      Safari/537.36
                      PTST/220609.133020
```

weather.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header.

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

https://adalytics.io/blog/prebid-bot-filtration


si.com/college-football/ohio-state-michigan-football-rivalry-needs-reset-after-postgame-melee
ON SI · SI SWIMSUIT · SI TICKETS · SI RESORTS · SI SHOPS · MY ACCOUNT · SUBSCRIBE NOW
SI
PRICE DROP
PRICE DROP
PRICE DROP
Switch to T-Mobile®
Network
35 3505 15
No throttling
Filter
Invert
More filters
All Fetch/XHR Doc CSS JS Font Img Media Manifest WS
Url
Headers Preview Response Initiator Timing
ht...
1 requ

John Cooper got 13 years as coach of the Buckeyes with a 2–10–1 record against Michigan. Harbaugh lost his first four against Ohio State as coach of the Wolverines, but got a chance to turn that around. Such patience seems unrealistic in the current toxic times.

Day is 66–10 at Ohio State, a ridiculous record, and yet it isn't good

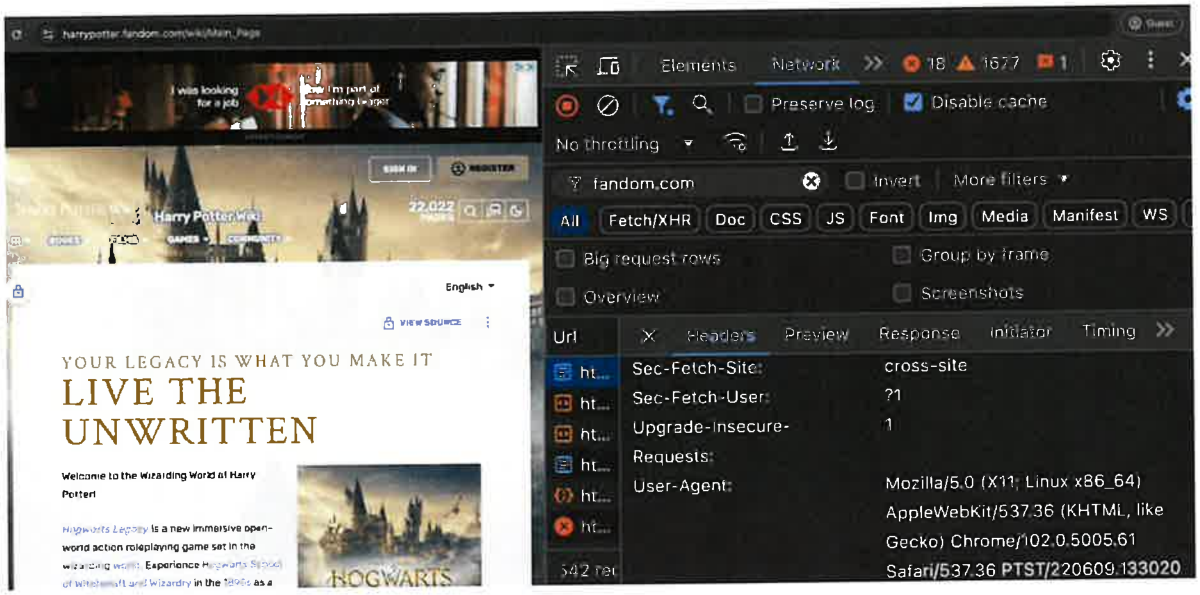
□ Preserve log ☑ Disable cache

□ Big request rows □ Group by frame

□ Overview □ Screenshots

Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020

Minute Media operated si.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header.



YOUR LEGACY IS WHAT YOU MAKE IT

LIVE THE UNWRITTEN

Welcome to the Wizarding World of Harry Potter!

Hogwarts Legacy is a new immersive open-world action roleplaying game set in the wizarding world. Experience Hogwarts School of Witchcraft and Wizardry in the 1800s as a

□ Preserve log ☑ Disable cache

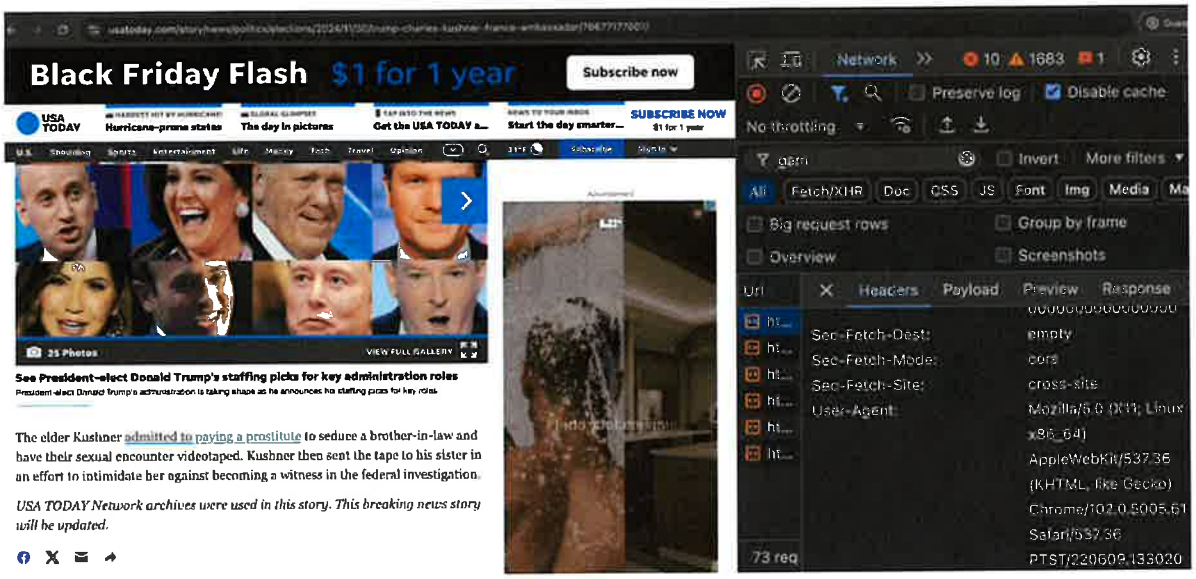
Filter: fandom.com

□ Big request rows □ Group by frame

□ Overview □ Screenshots

Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.61 Safari/537.36 PTST/220609.133020

fandom.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header. Fandom uses IAS and DoubleVerify publisher optimization tools on its pages.



See President-elect Donald Trump's staffing picks for key administration roles

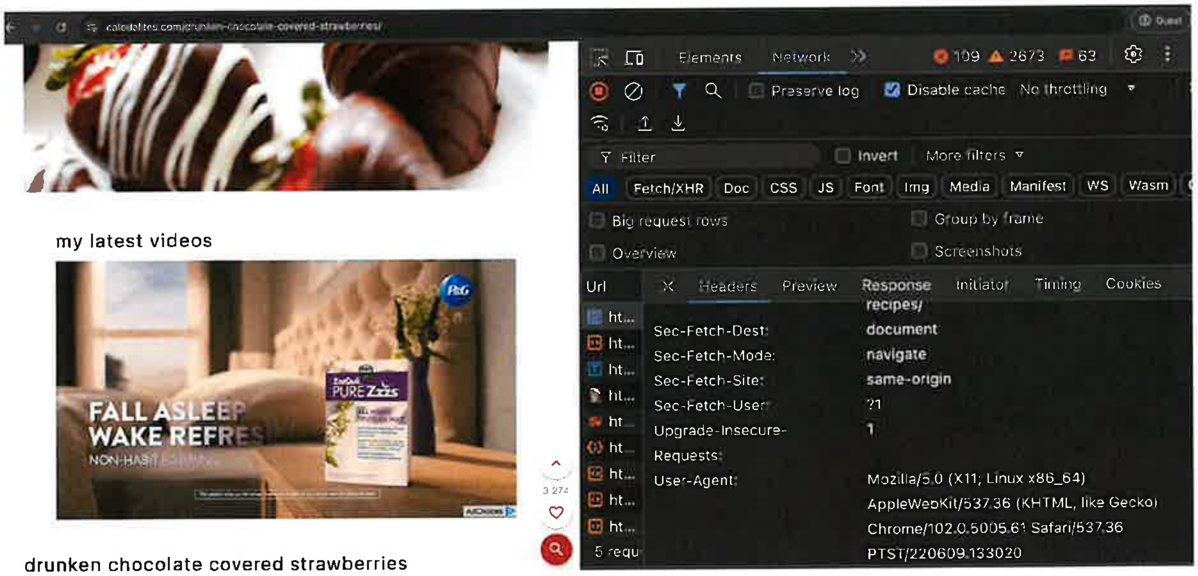
President-elect Donald Trump's administration is taking shape as he announces his staffing picks for key roles.

The elder Kushner admitted to paying a prostitute to seduce a brother-in-law and have their sexual encounter videotaped. Kushner then sent the tape to his sister in an effort to intimidate her against becoming a witness in the federal investigation.

USA TODAY Network archives were used in this story. This breaking news story will be updated.

```
Sec-Fetch-Dest:    empty
Sec-Fetch-Mode:    cors
Sec-Fetch-Site:    cross-site
User-Agent:        Mozilla/5.0 (X11; Linux
                   x86_64)
                   AppleWebKit/537.36
                   (KHTML, like Gecko)
                   Chrome/102.0.5005.61
                   Safari/537.36
                   PTST/220609.133020
```

Gannett Media operated usatoday.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header.



```
                           recipes/
Sec-Fetch-Dest:            document
Sec-Fetch-Mode:            navigate
Sec-Fetch-Site:            same-origin
Sec-Fetch-User:            ?1
Upgrade-Insecure-
Requests:                  1
User-Agent:                Mozilla/5.0 (X11; Linux x86_64)
                           AppleWebKit/537.36 (KHTML, like Gecko)
                           Chrome/102.0.5005.61 Safari/537.36
                           PTST/220609.133020
```

cafedelites.com appears to serve ads even if the user declares themself to be a bot via the HTTP User Agent request header. a P&G Vicks video ad can be seen in the screenshot.

Prompted by these observations, Adalytics reached out to several of the media publishers who appear to be filtering out declared bot traffic. Adalytics asked them for comments about how and why they are filtering out declared bot traffic, or preventing ads from serving to declared bots such as the HTTP Archive bot.

Several of the media publishers declined to respond or comment. However one publisher - the Arena Group, agreed to provide comments "on the record" that could be cited in this report.

The questions and answers can be seen below. The bolded text at the top represents questions that Adalytics asked, and the non-bolded text below contains the publisher's responses.

1. **What is Arena Group's position on serving ads to bots?**
   - *"We believe it's inappropriate to serve ads to bots. Therefore, we employ a significant amount of resources to ensure our traffic is high-quality. Advertisers chose to work with Arena because of our reach, influence and performance. Serving ads to bots is a betrayal of that trust and would only degrade our performance and relationships."*
2. **Do publishers have any responsibility in ensuring ads do not serve to bots, or should the responsibility lie with SSPs, DSPs, media agencies or brands' verification vendors?**
   - *"Dealing with bots and other types of fraud is the responsibility of every company in the advertising supply chain. No single solution is perfect, but, for us, it's very important to ensure our traffic is authentic.Therefore, we take additional steps to combat bot traffic and don't rely solely on one partner."*
3. **What is the "opportunity cost" for a publisher of forgoing serving ads to declared bots and data center-originating web traffic?**
   - *"In the long term, there is no real cost. While it may seem appealing for a publisher to show ads to bots and, therefore, drive traffic and revenue in the short term, it actually is a bad long-term decision. It creates noise or bad data, thereby potentially guiding us in the wrong direction. It also reduces trust with our advertising partners. When we build strategies based on our real traffic and revenue trends, we know we're making better decisions and providing real value for our partners for the long term."*
4. **For a publisher, what are the trade-offs when considering whether or not to allow ads to serve to bots on the publishers' properties?**

   - *"As mentioned, allowing ads to be served to bot traffic could enable additional short-term revenue, but not without significant downsides, not the least of which is creating a lot of noise in our data about consumer and revenue trends, but also decreased value for our advertisers. If advertisers can't trust us, they won't work with us."*

5. **How much bot traffic and data center-originated traffic does a publisher see on its properties? For example, do 5%, 10%, 15% of page visits come from bots?**
   - *"25-30% range and it can be as high as 40+%"*

Conclusion

Caveats & Limitations

Interpreting the results of this observational study requires nuance and caution.

The digital media supply chain has numerous stakeholders involved in transacting an ad. When a digital ad is delivered on a website, it can involve a publisher, one or more supply side platforms or ad exchanges, one or more ad servers, one or more verification vendors, a demand side platform, and/or a media agency. Thus, it can be difficult to determine or infer who was "responsible" or made a "decision" that resulted in an ad being served to a bot. Even if a vendor has correctly identified a user as a bot, sometimes other stakeholders may intentionally or inadvertently still authorize an ad to be served to that bot.

For example, a vendor may correctly identify a bot, and pass that information to another vendor who controls the ad serving or bidding decisioning process. That second vendor - for a number of reasons - may disregard, ignore, or fail to action the accurate and correct bot classification returned by the first vendor.

One should not assume that because a given ad tech vendor or vendors transacted a given ad to a bot that those vendors are somehow responsible or "at fault" for the ad being served to a bot. It is possible that a different stakeholder in the media supply chain ignored or accidentally 'over-rode' the recommendations or data points provided by other ad tech vendors, or that limited information was passed between vendors in the media supply chain.

The Results section of this report is based entirely on publicly available data obtained on the open web through open source intelligence (OSINT) techniques. None of the data, observations or analysis included in the Results section of this report came from privileged, non-public, or proprietary sources.

Readers should be discerning and careful not to conflate distinct sets of observations or draw inferences about causality, intent, quantitative impact, magnitude, or provenance.

For avoidance of doubt, this report makes no assertions about the above. This report makes no assertions about the intent behind certain media buying practices, and whether or not it was done with specific parties' authorization. This report makes no assertions or claims with regards to the quantitative magnitude of some of the phenomena observed in this study. This observational research study does not make any assertions regarding causality, provenance, intent, quantitative impact, or relative abundance.

This study does not make any recommendations to media buyers with regards to whether or not to transact with specific ad vendors or with specific publishers. The study is intended solely to present a set of public observations, so that readers can come to their own conclusions and make their own informed decisions.

Furthermore, this report is based on publicly accessible, client side forensics/strings. Those forensics can yield false positives, for example, in situations where an "adomain" or ad clickthrough URL destination is not indicative of who paid for a given ad placement.

Caveats & Limitations - Questions & Answers (Q&A)

1. **Does this study make any assertions with regards to quantitative impact?**

No. This study does not make any assertions with regards to quantitative impact. For example, this study does not quantify how many total ads were served via specific vendors to bots, or the absolute prevalence of bot traffic in digital advertising.

2. **Does this study recommend that media buyers exclude or block specific publishers or intermediaries from future ad buys?**

No. This study does not recommend or advise any media buyers to exclude or block specific vendors, intermediaries, or sellers from future ad buys. Each media buyer may wish to review their own ad buy records, their media buying requirements, and make their own informed decisions with regards to whether or not to continue to transact with any specific media vendor or intermediary.

3. **Does this study assert that any specific verification vendors, media agencies, DSPs, SSPs, vendors, intermediaries, suppliers, or sellers are "at fault" for specific potentially un-desired ad transactions?**

No. This observational research study makes no assertions with regards to fault, intent, or causality. In many cases it is not possible to fully attribute why a given ad was served, and there may be multiple different stakeholders involved. For example, many programmatic ads are transacted by a publisher that operates a website, a supply side platform, a demand side platform, a media agency, a publisher ad server, an advertiser ad server, and a verification vendor. One or more of these entities may have a role to play in why an ad was served at a given time.

Moreover, some of the vendors mentioned in this post provide limited information about how their solutions function, and no information about how their solutions are supposed to work in a transaction where every various parties are using some form of "filtration" by two different vendors.

Discussion

In 2018, two US Senators wrote a letter in 2018 to the Federal Trade Commission (FTC) "t*o express frustration with the growing phenomenon of digital ad fraud*" and asking the FTC to investigate:

"***the extent to which major ecosystem stakeholders engage in willful blindness to fraudulent activity in the online ad market.***"

The Financial Times previously cited Mikko Kotila, a computer scientist and co-author of a landmark World Federation of Advertisers (WFA) report on ad fraud, as saying:

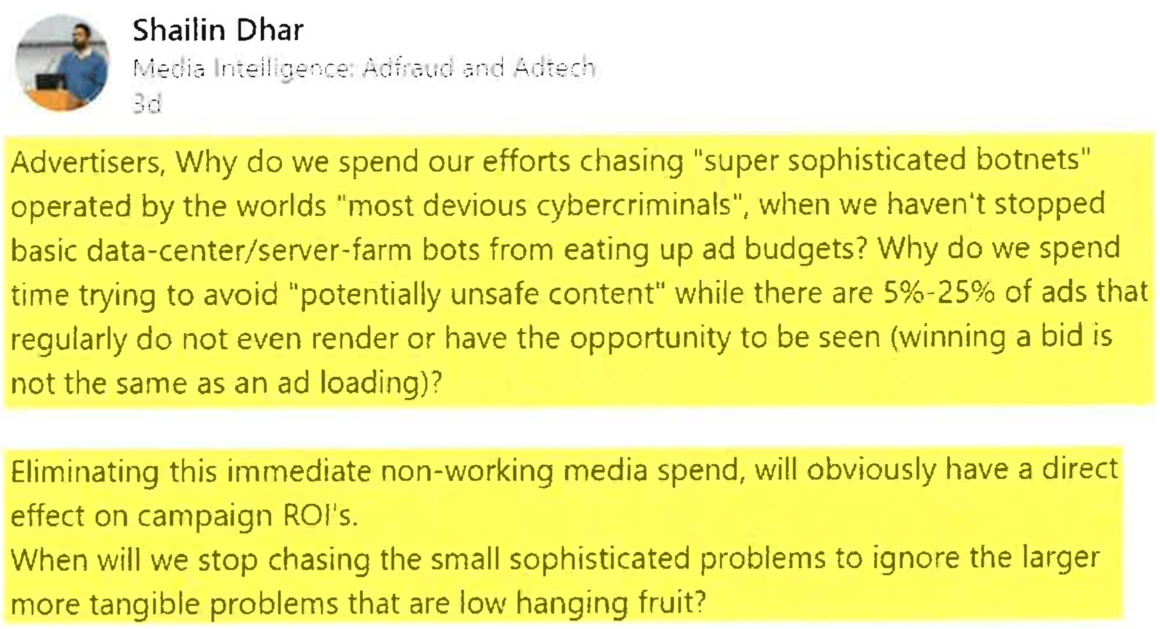
"Mr Kotila says middlemen in the digital media supply chain often turn a blind eye to fake traffic and other skulduggery because doing so is in their financial interest. "They are either ignorant of the fraud or they are an accomplice to it," he says."

The Financial Times previously cited Shailin Dhar, an ad tech industry expert, saying:

"Mr Dhar remains sceptical about how far the industry will get in its fraud-fighting efforts, given that many constituents have a financial incentive to maintain the status quo. "Ad tech companies have made billions of dollars a year from fraudulent traffic," he says. "Fraud is built into the foundation of advertising supply.""

Shailin Dhar previously commented in a Linkedin post: "

"Advertisers, Why do we spend our efforts chasing "super sophisticated botnets" operated by the worlds "most devious cybercriminals", when we haven't stopped basic data-center/server-farms from eating up ad budgets?"



Shailin Dhar
Media Intelligence: Adfraud and Adtech
3d

Advertisers, Why do we spend our efforts chasing "super sophisticated botnets" operated by the worlds "most devious cybercriminals", when we haven't stopped basic data-center/server-farm bots from eating up ad budgets? Why do we spend time trying to avoid "potentially unsafe content" while there are 5%-25% of ads that regularly do not even render or have the opportunity to be seen (winning a bid is not the same as an ad loading)?

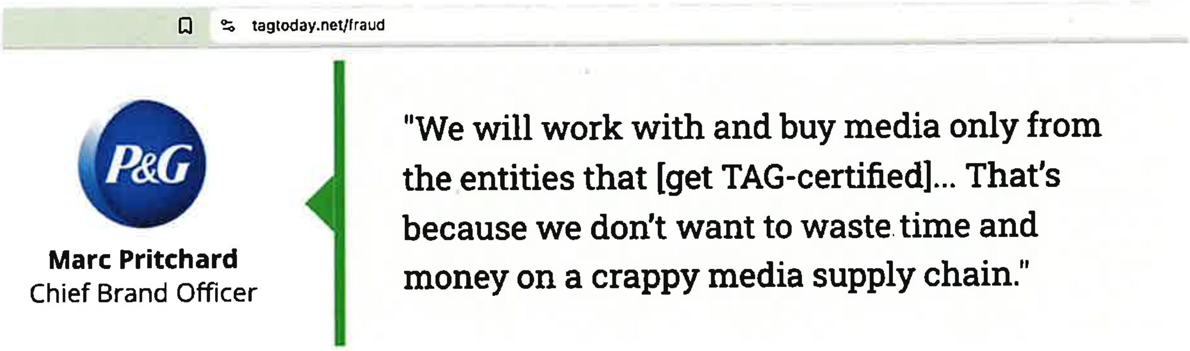
Eliminating this immediate non-working media spend, will obviously have a direct effect on campaign ROI's.
When will we stop chasing the small sophisticated problems to ignore the larger more tangible problems that are low hanging fruit?

Source: https://www.linkedin.com/pulse/marketers-stop-distracting-yourself-focus-ad-fraud/

The Association of National Advertisers (ANA) previously stated that:

"*A false sense of security enables fraud to thrive.*"

This research study documents how thousands of brands - including the United States federal government and military - had their ads served to bots. Some of the bots are openly declared bots whose user agent has been on the advertising industry's reference bot list since 2013, and were operating out of well known data center IP addresses.



Marc Pritchard
Chief Brand Officer

"We will work with and buy media only from the entities that [get TAG-certified]... That's because we don't want to waste time and money on a crappy media supply chain."

Screenshot of a quote from P&G Chief Brand Officer Marc Pritchard on the TAG website

Many of the ad tech vendors which appear to serve ads to bots claim to partner with vendors such as HUMAN Security. Some of these vendors made public claims that they are 100% of their prospective ad inventory with HUMAN, and ensuring ads are not served to bots. However, many of those ad tech - Trade Desk, Microsoft Xandr, Index Exchange, Google, Sovrn, Yieldmo, Sharethrough, Kargo, GumGum, Triplelift, Magnite, Pubmatic, Sonobi, Freewheel, media.net, Beachfront, Primis, and Omnicom Media Group were serving ads to bots.

Several of these vendors have made public statements about validating 100% of bid request pre-bid, and avoiding bidding on or serving ads to bots. However, this research shows that even vendors who made such public press releases were seen in some cases serving ads to bots.

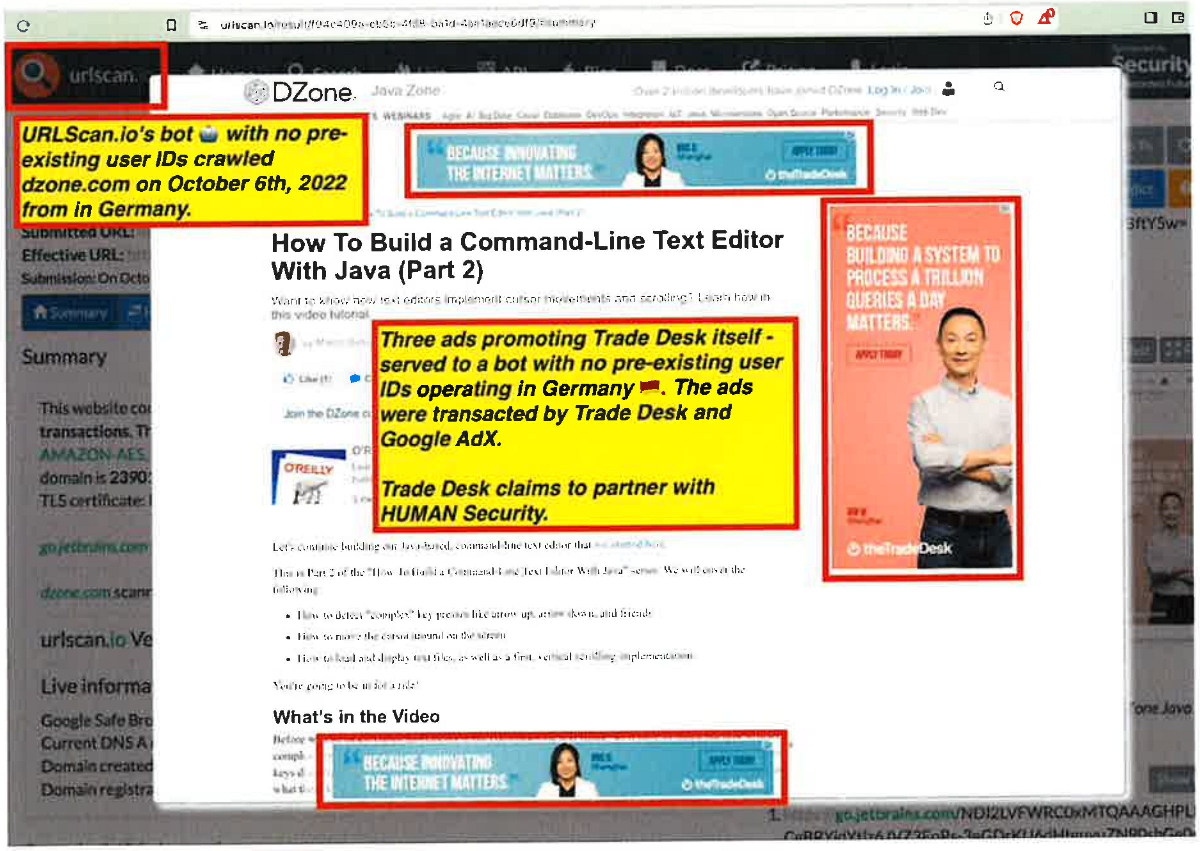
https://adalytics.io/blog/prebid-bot-filtration

Ad Tech Vendors & Agencies With Public Partnerships With **Human Security** (f/k/a 'White Ops') Who Transacted Ads to **Declared Bots** (Listed on the IAB Bots & Spiders List Since 2013) Operating From Known Data Center IPs

theTradeDesk
xandr
Index Exchange
Google
sovrn
yieldmo
sharethrough
KARGO
gumgum
triplelift
Magnite
PubMatic
sonobi
FREEWHEEL A COMCAST COMPANY
media.net
BEACHFRONT
[primis] Do Video Better
OMG Omnicom MediaGroup
tag

Denotes that this company has achieved the Trustworthy Accountability Group's **Certified Against Fraud** seal.

The Trade Desk had its own product and job recruiting ads served to bots in some cases.


urlscan.io
DZone
Java Zone
BECAUSE INNOVATING THE INTERNET MATTERS
APPLY TODAY
theTradeDesk
BECAUSE BUILDING A SYSTEM TO PROCESS A TRILLION QUERIES A DAY MATTERS
APPLY TODAY
Summary
urlscan.io Ve
Live informa
go.jetbrains.com/NDI2LVFWRC0xMTQAAAGHPL

URLScan.io's bot 🤖 with no pre-existing user IDs crawled dzone.com on October 6th, 2022 from in Germany.

How To Build a Command-Line Text Editor With Java (Part 2)

Want to know how text editors implement cursor movements and scrolling? Learn how in this video tutorial.

Three ads promoting Trade Desk itself - served to a bot with no pre-existing user IDs operating in Germany 🇩🇪. The ads were transacted by Trade Desk and Google AdX.

Trade Desk claims to partner with HUMAN Security.

Let's continue building our Java-based, command-line text editor that we started here.

This is Part 2 of the "How To Build a Command-Line Text Editor With Java" series. We will cover the following:

- How to detect "complex" key presses like arrow up, arrow down, and friends
- How to move the cursor around on the screen
- How to load and display text files, as well as a first, vertical scrolling implementation

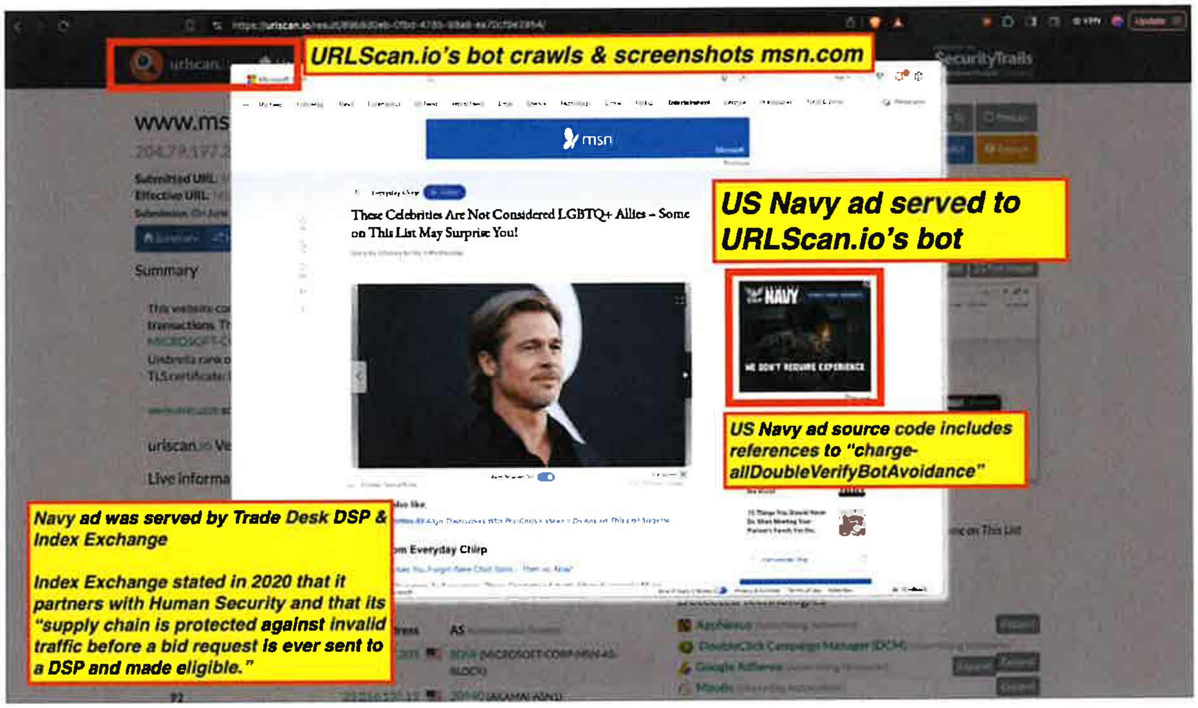
You're going to be in for a ride!

What's in the Video

[On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?](https://adalytics.io/blog/prebid-bot-filtration)

https://adalytics.io/blog/prebid-bot-filtration

Furthermore, many advertisers and media agencies appear to be utilizing the services of ad verification vendors Integral Ad Science and DoubleVerify, and having some of their ads served to bots. The source code of many brands' ads included references to "charge-allDoubleVerifyBotAvoidance" and "charge-allIntegralSuspiciousActivity". For example, the US Navy's ads included references to "charge-allDoubleVerifyBotAvoidance" and the US Postal Service's (USPS) ads included references to "charge-allIntegralSuspiciousActivity" when they were observing being served to bots. Some of these advertisers may be specifically paying for bot avoidance pre-bid segments.



URLScan.io's bot crawls & screenshots msn.com

US Navy ad served to URLScan.io's bot

US Navy ad source code includes references to "charge-allDoubleVerifyBotAvoidance"

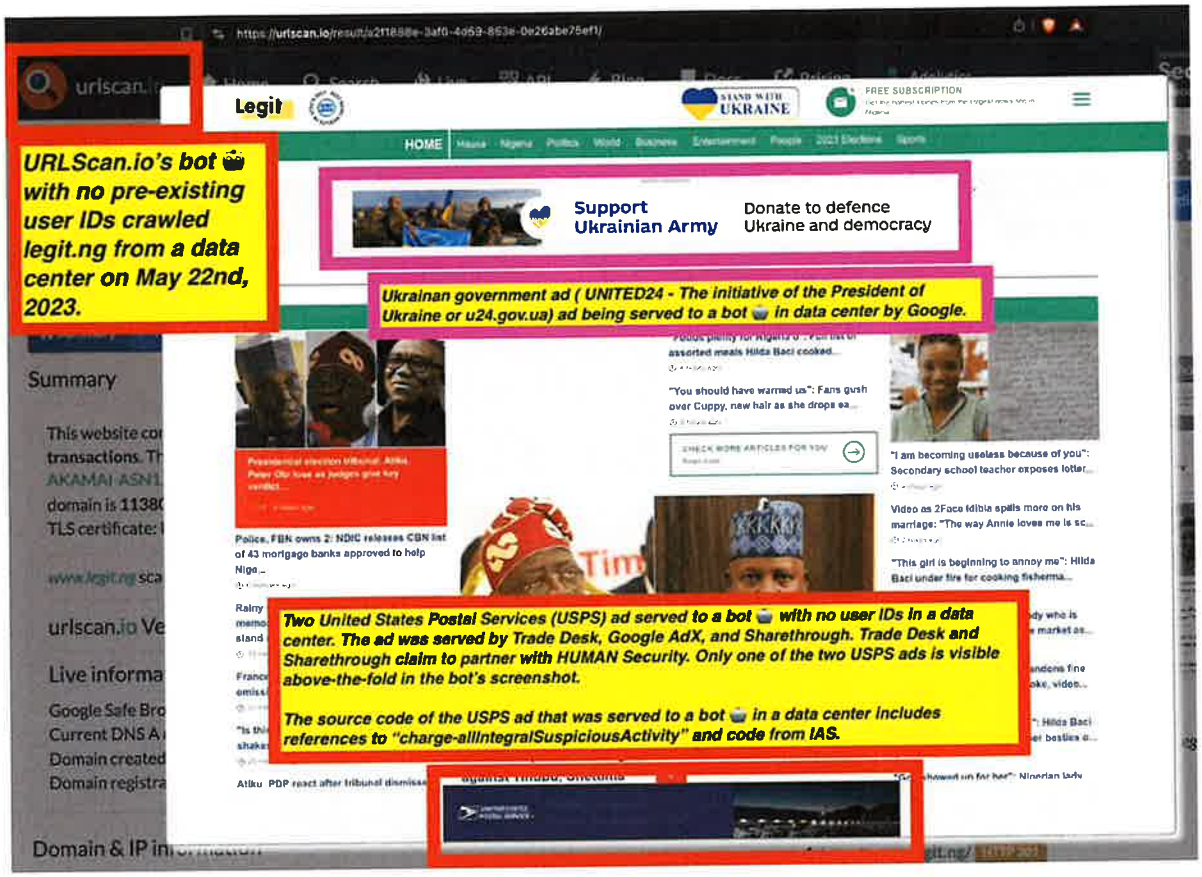
Navy ad was served by Trade Desk DSP & Index Exchange

Index Exchange stated in 2020 that it partners with Human Security and that its "supply chain is protected against invalid traffic before a bid request is ever sent to a DSP and made eligible."

urlscan.io
www.ms
msn
These Celebrities Are Not Considered LGBTQ+ Allies – Some on This List May Surprise You!
NAVY
WE DON'T REQUIRE EXPERIENCE
SecurityTrails
Summary
Live informa

On pre-bid bot detection and filtration - Are ad tech vendors serving US Government and Fortune 500 brands' digital ads to bots?

https://adalytics.io/blog/prebid-bot-filtration

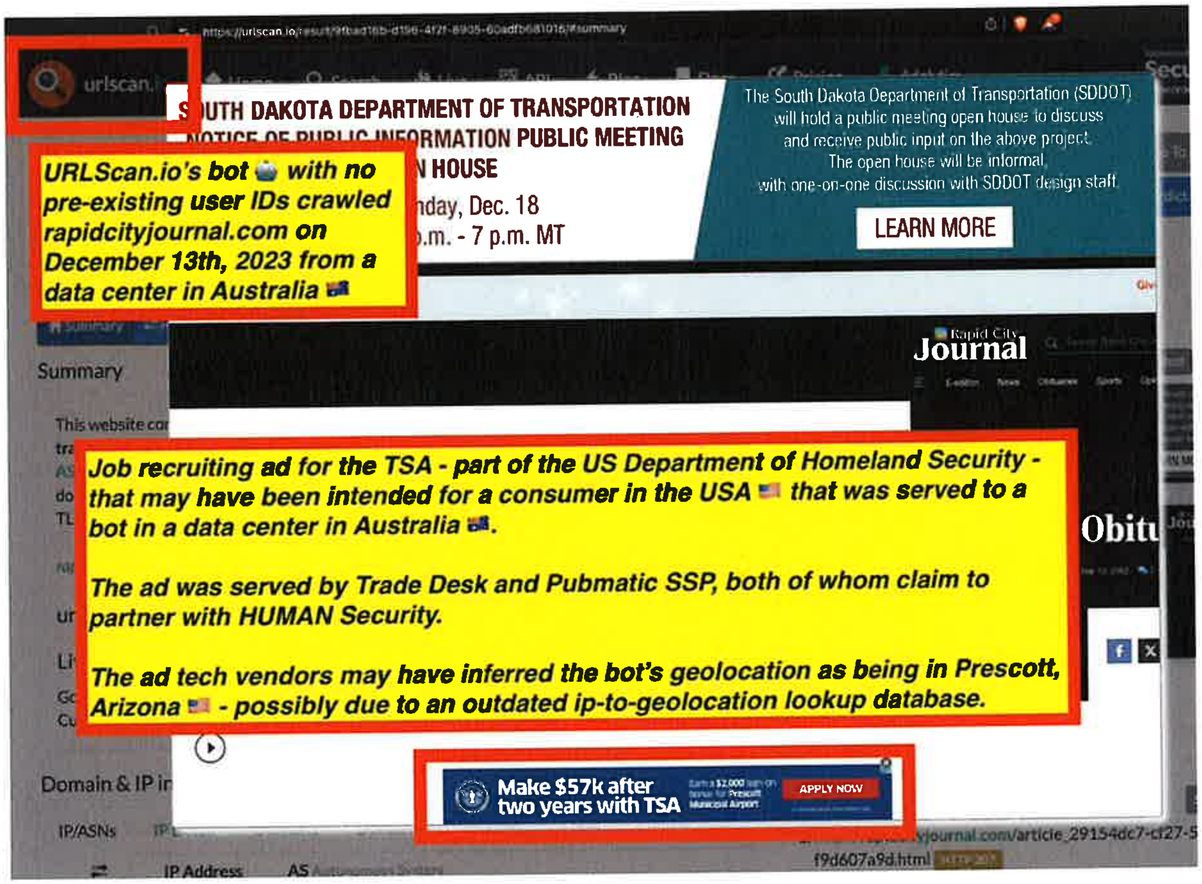


URLScan.io's bot 🤖 with no pre-existing user IDs crawled legit.ng from a data center on May 22nd, 2023.

Ukrainan government ad (UNITED24 - The initiative of the President of Ukraine or u24.gov.ua) ad being served to a bot 🤖 in data center by Google.

Two United States Postal Services (USPS) ad served to a bot 🤖 with no user IDs in a data center. The ad was served by Trade Desk, Google AdX, and Sharethrough. Trade Desk and Sharethrough claim to partner with HUMAN Security. Only one of the two USPS ads is visible above-the-fold in the bot's screenshot.

The source code of the USPS ad that was served to a bot 🤖 in a data center includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.


urlscan.
S UTH DAKOTA DEPARTMENT OF TRANSPORTATION
NOTICE OF PUBLIC INFORMATION PUBLIC MEETING
N HOUSE
nday, Dec. 18
.m. - 7 p.m. MT
The South Dakota Department of Transportation (SDDOT) will hold a public meeting open house to discuss and receive public input on the above project. The open house will be informal, with one-on-one discussion with SDDOT design staff.
LEARN MORE
Summary
Rapid City Journal
Obitu
Domain & IP in
IP/ASNs
IP Address
AS
Make $57k after two years with TSA
APPLY NOW
journal.com/article_29154dc7-cf27-5
f9d607a9d.html

*URLScan.io's **bot** 🤖 with **no** pre-existing **user** IDs crawled rapidcityjournal.com **on** December **13th**, 2023 from **a** data center in Australia 🇦🇺*

Job recruiting ad for the TSA - part of the US Department of Homeland Security - that may have been intended for a consumer in the USA 🇺🇸 that was served to a bot in a data center in Australia 🇦🇺.

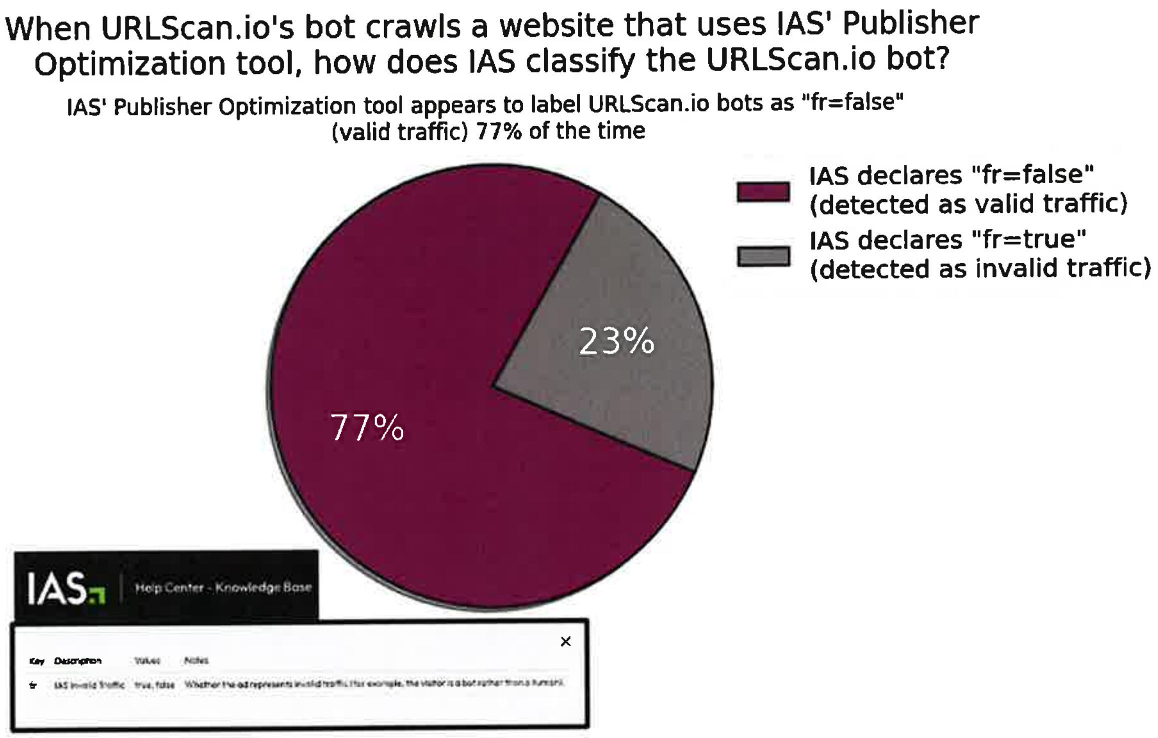
The ad was served by Trade Desk and Pubmatic SSP, both of whom claim to partner with HUMAN Security.

The ad tech vendors may have inferred the bot's geolocation as being in Prescott, Arizona 🇺🇸 - possibly due to an outdated ip-to-geolocation lookup database.

All major media agency holding companies - including IPG, Dentsu, Havas, Publicis Groupe, GroupM/WPP, and Omnicom, as well as MiQ and other agencies - were observed as transacting bot traffic. The World Federation of Advertisers (WFA) recommends that *"Contracts with agencies and vendor partners need to be revised to ensure that there are clear penalties for misallocating spend to ad fraud related inventory, where preventing it could be reasonably achieved."*

Many major media publishers who appear to have installed the IAS and/or DoubleVerify publisher optimization tools on their webpages were also seen serving ads to bots. For example, the Washington Post, Wall Street Journal, CNN, Weather.com, The Guardian, USA Today, Fandom, and Conde Nast were seen serving ads to bots whilst having IAS or DoubleVerify publisher optimization code configured on their pages.

Across the sample of URLScan.io crawls from 2019-2024, IAS's Publisher Optimization tool labeled the URLScan.io bot as valid, human traffic 77% of the time.



When URLScan.io's bot crawls a website that uses IAS' Publisher Optimization tool, how does IAS classify the URLScan.io bot?

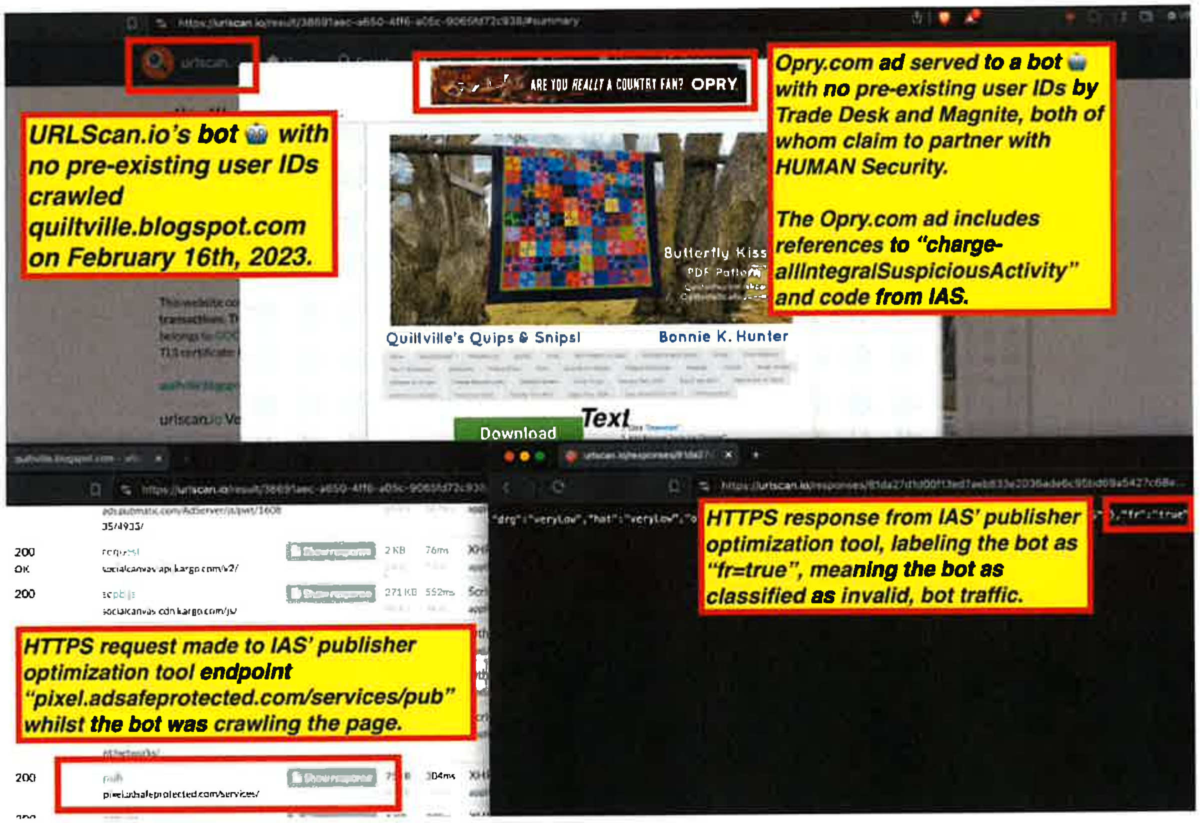
IAS' Publisher Optimization tool appears to label URLScan.io bots as "fr=false" (valid traffic) 77% of the time

Key	Description	Values	Notes
fr	IAS Invalid Traffic	true, false	Whether the ad represents invalid traffic (for example, the visitor is a bot rather than a human).

In some cases, it appears that IAS' publisher optimization tool labeled the same bot and page view session as both valid, human traffic ("fr=false") and simultaneously as invalid, bot traffic ("fr=true").

Furthermore, in some cases, even when IAS' publisher optimization tool identified a given user as a bot, there were still ads served to the bot on behalf of advertisers who appeared to be using IAS' advertiser-side tools.

https://adalytics.io/blog/prebid-bot-filtration


ARE YOU REALLY A COUNTRY FAN? OPRY
Quiltville's Quips & Snips!
Bonnie K. Hunter
Butterfly Kiss
Download
Text

URLScan.io's bot 🤖 with no pre-existing user IDs crawled quiltville.blogspot.com on February 16th, 2023.

Opry.com ad served to a bot 🤖 with no pre-existing user IDs by Trade Desk and Magnite, both of whom claim to partner with HUMAN Security.

The Opry.com ad includes references to "charge-allIntegralSuspiciousActivity" and code from IAS.

HTTPS response from IAS' publisher optimization tool, labeling the bot as "fr=true", meaning the bot as classified as invalid, bot traffic.

HTTPS request made to IAS' publisher optimization tool endpoint "pixel.adsafeprotected.com/services/pub" whilst the bot was crawling the page.

On February 16th, 2023, URLScan.io's bot visited quiltville.blogspot.com, and the IAS publisher optimization tool (via endpoint "pixel.adsafeprotected.com/services/pub") was invoked.. The IAS API endpoint returned the classification "fr=true", indicating invalid, bot traffic. An ad for Grande Ole Opry music stage in Nashville, Tennessee was served to the bot by Trade Desk and Magnite. The source code of the Opry ad that was served to a bot after IAS's tool labeled the page view as "fr=true" indicated "charge-allIntegralSuspiciousActivity". Source: https://urlscan.io/result/38691aec-a650-4ff6-a05c-9065fd72c938/#summary

The source code of ads from brands such as Progressive Insurance and the Government of Ontario, Canada included references to "Scibids", whilst those ads were served to bots with no pre-existing user IDs.

Whilst it is ostensibly possible that brands were not charged for some of the ads served to bots, analysis of data provided by advertisers in some cases suggests that the brands were in fact invoiced for ads served to bot traffic.

Some brands and agencies do not get access to high granularity impression level log file data with IP address, user agent, and user ID information. In those cases, it can be difficult if not outright impossible for the media buyers to assess how much they were invoiced for ads served to bots.

However, regardless of the financial impact of the digital ads that are served to bots, these bots can increase advertisers' Scope3 carbon emissions and lead to increased electricity consumption. Furthermore, the ads delivery can result in skewed or erroneous web analytics data that biases media investment decisions.

The World Federation of Advertisers (WFA) recommends that "*brands need to develop in-house expertise to support vendor selection, work with cyber security partners to help understand common threats and demand full transparency of investment*". The Association of National Advertisers (ANA) recommends that advertisers "*refuse payment on non-human traffic in media contracts.*"

Many advertisers - such as the New York City Police, Department of Homeland Security, the United States Navy, Army, Department of Veterans Affairs, HHS, healthcare.gov, CDC, USPS, the Federal Government of Germany, Australian Defence Force, Singaporean Police, Ontario Government, and governments of Utah, California, Virginia, Florida, New York, and Indiana - may benefit from undertaking a closer review of their digital advertising.